Alexander Gewirtz

Mathématiques Supérieures

Cours – tome 1

edp sciences

Dans la même collection

Éléments d'analyse réelle, 2e édition
Jean-Étienne Rombaldi
2019, ISBN : 978-2-7598-2339-0

Thèmes pour l'agrégation de mathématiques, 2e édition
Jean-Étienne Rombaldi
2019, ISBN : 978-2-7598-2340-6

Analyse matricielle – Cours et exercices résolus, 2e édition
Jean-Étienne Rombaldi
2019, ISBN : 978-2-7598-2341-3

Mathématiques Supérieures – Cours, tome 2
Alexander Gewirtz
2023, ISBN : 978-2-7598-2789-3

Imprimé en France

ISBN (papier) : 978-2-7598-2787-9 - ISBN (ebook) : 978-2-7598-2788-6

Tous droits de traduction, d'adaptation et de reproduction par tous procédés, réservés pour tous pays. La loi du 11 mars 1957 n'autorisant, aux termes des alinéas 2 et 3 de l'article 41, d'une part, que les « copies ou reproductions strictement réservées à l'usage privé du copiste et non destinées à une utilisation collective », et d'autre part, que les analyses et les courtes citations dans un but d'exemple et d'illustration, « toute représentation intégrale, ou partielle, faite sans le consentement de l'auteur ou de ses ayants droit ou ayants cause est illicite » (alinéa 1er de l'article 40). Cette représentation ou reproduction, par quelque procédé que ce soit, constituerait donc une contrefaçon sanctionnée par les articles 425 et suivants du code pénal.

© EDP Sciences, 2023

Préface et remerciements

Cet ouvrage est inspiré des cours de mathématiques proposés aux élèves-ingénieurs de l'Institut franco-chinois de l'énergie nucléaire (IFCEN), situé sur le campus de l'université Sun Yat-sen à Zhuhai, dans la province du Guangdong en Chine du Sud.

Les contenus mathématiques qui sont abordés à l'IFCEN correspondent quasiment au programme des classes préparatoires en France. Le programme de mathématiques de l'IFCEN a été conçu sous la direction de MM. Jacques Moisan et Charles Torossian, inspecteurs généraux de l'Éducation nationale, et adapté aux besoins des élèves-ingénieurs de l'IFCEN. Il est donc possible que quelques chapitres de ce livre ne soient pas étudiés en CPGE en France. Inversement, certains chapitres traditionnellement étudiés en France n'y sont pas abordés ou le sont de façon moins approfondie.

Dans le souci de rendre plus actif le lecteur pendant son apprentissage, de nombreuses questions et exercices d'applications sont posés dans le corps du texte, permettant de vérifier la maîtrise des formules et des concepts nouvellement acquis. Par ailleurs, les démonstrations, très complètes et détaillées, permettent au lecteur de bien suivre et de mieux comprendre à la fois la démonstration et ses idées. De plus, celui-ci peut faire le point sur son apprentissage grâce à de nombreux bilans méthodologiques. Une large sélection d'exercices (de difficulté variable) est proposée à la fin de chaque chapitre, permettant ainsi de pratiquer ce qui a été appris et proposant parfois une ouverture sur des sujets plus avancés. Enfin, certaines démonstrations de théorèmes admis et certains compléments figurent en annexe de certains chapitres pour les lecteurs qui souhaiteraient approfondir leurs connaissances mathématiques.

Les livres de cette collection sont en constante évolution, grâce aux remarques et aux suggestions des élèves et des professeurs de l'institut. J'ai plaisir à mentionner mes collègues les docteurs Alexis Gryson et Cheng Sirui, pour la relecture minutieuse des manuscrits. La collection n'aurait pas pu voir le jour sans les encouragements et le soutien constant des deux directeurs de l'institut : professeur Wang Biao et M. Jean-Marie Bourgeois-Demersay. Qu'ils en soient tous ici remerciés !

Un grand merci à mon épouse et mes enfants pour leur soutien constant !

Enfin, je remercie à titre personnel François Boisson sans lequel je ne serais jamais devenu professeur de mathématiques.

Alexander Gewirtz

Table des matières

Chapitre 1 Groupes, anneaux et corps **7**
1.1 Groupes . . . 8
1.1.1 Loi de composition interne . . . 8
1.1.2 Définition d'un groupe et règles de calcul . . . 13
1.1.3 Sous-groupes . . . 18
1.1.4 Opérations sur les sous-groupes . . . 20
1.1.5 Morphismes de groupes . . . 22
1.2 Anneaux et corps . . . 28
1.2.1 Définitions . . . 28
1.2.2 Sous-anneaux et sous-corps . . . 29
1.2.3 Règles de calcul dans un anneau . . . 32
1.2.4 Opérations sur les sous-anneaux et sous-corps . . . 36
1.2.5 Morphismes d'anneaux (ou de corps) . . . 37
1.3 Exercices . . . 41

Chapitre 2 Relations, ensembles $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$ et $\mathbb{R}$ **47**
2.1 Relations . . . 48
2.1.1 Généralités sur les relations . . . 48
2.1.2 Relation d'ordre . . . 50
2.1.2.a Ordre total et ordre partiel . . . 52
2.1.2.b Majorant, minorant, plus grand et plus petit élément . . . 53
2.1.2.c Borne supérieure et borne inférieure . . . 56
2.1.2.d Applications croissantes, décroissantes et monotones . . . 58
2.1.3 Relation d'équivalence . . . 60
2.2 Ensemble $\mathbb{N}$ et principe de récurrence . . . 61
2.2.1 Définition de l'ensemble $\mathbb{N}$ . . . 61
2.2.2 Principe de récurrence . . . 62
2.2.2.a Récurrence simple . . . 62
2.2.2.b Récurrence double . . . 65
2.2.2.c Récurrence forte . . . 66
2.2.2.d Récurrence finie et récurrence descendante . . . 67
2.3 Ensemble $\mathbb{Z}$ et valeur absolue . . . 69
2.3.1 Ensemble $\mathbb{Z}$ et structure d'anneau . . . 69
2.3.2 Valeur absolue dans $\mathbb{Z}$ . . . 71

2.4 Ensembles des nombres réels . . . 71
2.4.1 Corps des nombres rationnels . . . 71
2.4.2 Corps des nombres réels et relation d'ordre . . . 72
2.4.3 Valeur absolue . . . 72
2.4.4 Propriétés de la borne supérieure et de la borne inférieure . . . 75
2.4.5 Partie entière . . . 79
2.4.6 Caractérisation des intervalles de $\mathbb{R}$ . . . 81
2.4.7 Droite numérique achevée . . . 84
2.4.8 Densité de $\mathbb{Q}$ et de $\mathbb{R} \setminus \mathbb{Q}$ . . . 84
2.4.9 Valeurs décimales approchées d'un nombre réel . . . 87
2.5 Exercices . . . 88
2.6 Annexe . . . 96
2.6.1 Construction de $\mathbb{Z}$ . . . 96
2.6.2 Ensembles finis et dénombrements . . . 105
2.6.2.a Définitions et théorème fondamental . . . 105
2.6.2.b Parties de $\mathbb{N}$ et parties d'un ensemble fini . . . 109
2.6.2.c Critère de bijection pour les ensembles finis . . . 114
2.6.2.d Dénombrement . . . 117
2.6.2.e Cardinal d'une réunion et du complémentaire d'une partie 117
2.6.2.f Produit cartésien . . . 117
2.6.2.g Ensemble des applications de E vers F . . . 118
2.6.2.h Cardinal de $\mathcal{P}(E)$ . . . 119
2.6.2.i Arrangements, nombres d'injections et nombres de bijections d'un ensemble dans lui-même . . . 121
2.6.2.j Combinaisons et coefficients binomiaux . . . 123
2.6.2.k Propriétés des coefficients binomiaux . . . 124

Chapitre 3 Suites de nombres réels ou complexes 125
3.1 Suites de nombres réels . . . 126
3.1.1 Généralités . . . 126
3.1.2 Opérations sur les suites . . . 129
3.1.3 Suites extraites . . . 134
3.2 Suites définies par une relation de récurrence . . . 135
3.2.1 Suites arithmétiques et géométriques . . . 136
3.2.2 Notations Σ et Π . . . 137
3.2.3 Suites récurrentes linéaires d'ordre 2 à coefficients constants . . . 142
3.3 Limite d'une suite . . . 150
3.3.1 Convergence vers un réel ℓ : définition et propriétés . . . 150
3.3.2 Convergence et signe . . . 154
3.3.3 Divergence d'une suite . . . 155
3.3.3.a Divergence vers $+\infty$ ou vers $-\infty$ . . . 156
3.3.3.b Autres modes de divergence . . . 157
3.3.4 Opérations sur les suites convergentes . . . 158

3.3.4.a Espace vectoriel des suites convergeant vers 0 158
3.3.4.b Opérations algébriques sur les limites 160
3.3.5 Compatibilité du passage à la limite avec la relation d'ordre 164
3.3.6 Convergence et suites extraites 169
3.3.7 Caractérisation de la densité par les suites 173
3.4 Théorèmes d'existence de limite 174
3.4.1 Théorèmes de convergence et de divergence monotone 174
3.4.2 Application du théorème de la limite monotone aux séries à termes positifs 178
3.4.3 Théorème des suites adjacentes et théorème des segments emboîtés 187
3.4.4 Théorème de Bolzano-Weierstrass 190
3.5 Relations de comparaison 192
3.5.1 Suites dominées ou négligeables par rapport à une autre 192
3.5.2 Suites équivalentes 193
3.5.3 Comparaison des suites de référence 198
3.5.4 Développement asymptotique d'une suite 199
3.6 Suites à valeurs complexes 202
3.6.1 Définitions et convergence d'une suite complexe 202
3.6.2 Lien avec les parties réelle et imaginaire 204
3.7 Exercices 205

Chapitre 4 Espaces vectoriels et applications linéaires 215
4.1 Espaces vectoriels 216
4.1.1 Définition et exemples usuels 216
4.1.2 Règles de calcul dans un espace vectoriel 219
4.1.3 Sous-espaces vectoriels 221
4.2 Opérations sur les espaces vectoriels 225
4.2.1 Intersection et sous-espace engendré par une partie 225
4.2.2 Somme de sous-espaces vectoriels 232
4.2.3 Sommes directes et sous-espaces vectoriels supplémentaires 236
4.2.4 Produit cartésien de deux espaces vectoriels 241
4.3 Sous-espaces affines 243
4.3.1 Translations et groupes des translations d'un espace vectoriel 243
4.3.2 Définition d'un sous-espace affine 244
4.3.3 Parallélisme 247
4.3.4 Intersection de deux sous-espaces affines 248
4.4 Applications linéaires 249
4.4.1 Définition et exemples 249
4.4.2 Noyau et image d'une application linéaire 253
4.4.3 Équations linéaires 258
4.4.4 Ensembles des applications linéaires $\mathcal{L}(E, F)$ 259
4.4.5 Isomorphismes, automorphismes et groupe linéaire 263
4.4.6 Restriction et recollement 265

4.4.7 Hyperplans d'un espace vectoriel et formes linéaires . . . 268
4.4.8 Étude d'applications linéaires remarquables . . . 271
4.4.8.a Homothéties . . . 271
4.4.8.b Projecteurs . . . 272
4.4.8.c Symétries . . . 276
4.5 Exercices . . . 279

Chapitre 5 Arithmétique dans $\mathbb{Z}$ 287
5.1 Arithmétique dans $\mathbb{Z}$ . . . 288
5.1.1 Diviseurs et congruences . . . 288
5.1.2 Nombres premiers et décomposition en produit de facteurs premiers 291
5.1.3 Division euclidienne . . . 294
5.1.4 Sous-groupes de $(\mathbb{Z}, +)$ . . . 295
5.1.5 Plus grand commun diviseur et plus petit commun multiple . . . 296
5.1.6 Théorème de Bézout et algorithme d'Euclide . . . 298
5.1.7 Lemme d'Euclide et théorème de Gauss . . . 302
5.2 Exercices . . . 308
5.3 Annexe . . . 310
5.3.1 Anneaux $\mathbb{Z}/n\mathbb{Z}$ et quelques propriétés . . . 310
5.3.2 Corps $\mathbb{Z}/p\mathbb{Z}$ et éléments inversibles de $\mathbb{Z}/n\mathbb{Z}$ . . . 312

Chapitre 6 Fonctions réelles ou complexes d'une variable réelle 313
6.1 Généralités sur les fonctions d'une variable réelle . . . 314
6.1.1 Ensemble $\mathcal{F}(I, \mathbb{K})$ et relation d'ordre . . . 314
6.1.2 Ensemble $\mathcal{B}(I, \mathbb{K})$ . . . 315
6.1.3 Fonctions périodiques . . . 317
6.1.4 Fonctions paires et fonctions impaires . . . 318
6.1.5 Fonctions lipschitziennes . . . 320
6.1.6 Fonctions monotones . . . 322
6.2 Étude locale d'une fonction . . . 323
6.2.1 Voisinage d'un point . . . 323
6.2.2 Limite d'une fonction en un point et continuité en un point . . . 325
6.2.3 Opérations algébriques sur les limites . . . 335
6.2.4 Compatibilité du passage à la limite avec la relation d'ordre dans $\mathbb{R}$ 341
6.2.5 Composition de limites et caractérisation séquentielle de la limite . 348
6.2.6 Théorème de la limite monotone . . . 353
6.3 Relations de comparaisons . . . 356
6.3.1 Fonctions dominées et fonctions négligeables par rapport à une autre au voisinage d'un point . . . 356
6.3.2 Comparaison des fonctions usuelles . . . 363
6.3.3 Fonctions équivalentes en un point . . . 364
6.3.4 Équivalents usuels . . . 368
6.4 Continuité globale . . . 372

6.4.1 Définition et premières propriétés . . . 372
6.4.2 Composée de deux fonctions continues . . . 374
6.4.3 Restriction et caractère « local » de la continuité . . . 375
6.4.4 Prolongement par continuité . . . 376
6.4.5 Théorème des valeurs intermédiaires . . . 378
6.4.6 Image d'un segment par une fonction continue . . . 381
6.4.7 Continuité de la bijection réciproque . . . 383
6.4.8 Continuité uniforme et théorème de Heine . . . 384
6.5 Bilan sur les différences entre fonctions à valeurs réelles ou complexes . . . 389
6.6 Exercices . . . 391

Chapitre 7 Polynômes et fractions rationnelles 396
7.1 Ensemble $\mathbb{K}[X]$ . . . 397
7.1.1 Algèbres et morphisme d'algèbres . . . 397
7.1.2 Définition d'un polynôme . . . 401
7.1.3 Opérations usuelles sur les polynômes . . . 401
7.1.4 Dérivation sur l'ensemble des polynômes . . . 409
7.2 Degré d'un polynôme . . . 412
7.2.1 Définition . . . 412
7.2.2 Propriétés du degré . . . 413
7.2.3 Conséquences fondamentales . . . 414
7.3 Arithmétique dans $\mathbb{K}[X]$ . . . 415
7.3.1 Divisibilité dans $\mathbb{K}[X]$ . . . 415
7.3.2 Division euclidienne dans $\mathbb{K}[X]$ . . . 419
7.3.3 Idéaux de $\mathbb{K}[X]$ . . . 423
7.3.4 Polynômes premiers entre eux . . . 425
7.3.5 Théorème de Bézout et théorème de Gauss . . . 427
7.4 Racines d'un polynôme . . . 429
7.4.1 Fonction polynomiale associée à un polynôme . . . 429
7.4.2 Racines d'un polynôme . . . 430
7.4.3 Formule de Taylor et multiplicité d'une racine . . . 432
7.4.4 Méthodes pour montrer que deux polynômes sont égaux . . . 436
7.4.5 Polynômes scindés et relations entre racines et coefficients . . . 437
7.5 Polynômes irréductibles et factorisation . . . 439
7.5.1 Éléments irréductibles dans $\mathbb{C}[X]$ . . . 440
7.5.2 Éléments irréductibles dans $\mathbb{R}[X]$ . . . 441
7.6 Ensemble $\mathbb{K}(X)$ . . . 442
7.6.1 Corps des fractions rationnelles $\mathbb{K}(X)$ . . . 442
7.6.2 Dérivation et degré . . . 443
7.6.3 Zéros et pôles d'une fraction rationnelle . . . 445
7.6.4 Décomposition en éléments simples . . . 446
7.7 Exercices . . . 448

Chapitre 1

Groupes, anneaux et corps

Prérequis : dans tout ce chapitre, les notions suivantes sont supposées connues :

- le cours de logique (en particulier, implications et équivalences) ;
- notion d'ensemble et opérations usuelles sur les ensembles ;
- image directe et image réciproque d'une partie par une application ;
- composition d'applications, propriétés de la composition ;
- injection, surjection, bijection et leurs propriétés ;
- produit scalaire et déterminant dans le plan et dans l'espace, produit vectoriel dans l'espace.

Vous connaissez depuis longtemps l'addition et la multiplication de nombres réels (ou de nombres entiers). En fait, vous avez appris que ce sont des opérations qui ont un certain nombre de règles de calculs. Dans ce chapitre, on va généraliser ces « opérations » (ce qu'on appellera des lois de composition interne) et les règles de calcul. Ceci va nous amener à définir des notions de structures algébriques : notions fondamentales en mathématiques qui permettent essentiellement de manipuler des objets (des nombres, des ensembles, des applications, des vecteurs...) et de faire des « calculs » avec ces objets.

Vous verrez par la suite que ces structures reviennent naturellement dans tous les domaines mathématiques, mais aussi dans tous les domaines scientifiques.

1.1 Groupes

1.1.1 Loi de composition interne

Définition 1.1.1.1 Soit E un ensemble non vide. On appelle loi de composition interne sur E toute application $f : E \times E \longrightarrow E$. La valeur $f(x, y)$ pour un couple $(x, y) \in E^2$ s'appelle le composé de x et y pour cette loi.

Exemple 1.1.1.2 Voici quelques exemples et contre-exemples de lois de composition interne :

- l'addition sur $\mathbb{N}$ est une loi de composition interne ;
- la multiplication dans $\mathbb{C}$ est une loi de composition interne sur $\mathbb{C}$;
- si E est un ensemble donné, alors $\cup$ est une loi de composition interne sur $\mathcal{P}(E)$;
- le produit vectoriel $\wedge$ est une loi de composition interne sur $\mathbb{R}^3$;
- la loi $\circ$ est une loi de composition interne sur $\mathcal{F}(E, E)$ mais n'est pas une loi de composition interne sur $\mathcal{F}(E, F)$ (lorsque E et F sont deux ensembles distincts) ;
- par contre, le déterminant dans le plan n'est pas une loi de composition interne : à deux vecteurs, on associe un nombre réel et non pas un vecteur.

Notations :

- on utilise souvent l'expression « l.c.i. » pour dire « loi de composition interne ». C'est une abréviation qui est tolérée ;
- en général, on utilise un symbole pour désigner le composé de x et y, comme par exemple $x \star y$, ou xTy, ou $x \diamond y$, ou... On dira donc souvent : « soit $\star$ une loi de composition interne sur E » (au lieu de f) et on notera $x \star y$ au lieu de $f(x, y)$.

Définition 1.1.1.3 Soient E un ensemble non vide et $\star$ une loi de composition interne sur E. On dit que :

- $\star$ est associative si : $\forall (x,y,z) \in E^3$, $x \star (y \star z) = (x \star y) \star z$;
- $\star$ est commutative si : $\forall (x,y) \in E^2$, $x \star y = y \star x$;
- $\star$ possède un élément neutre s'il existe $e \in E$ tel que $\forall x \in E$, $e \star x = x \star e = x$.

Exemple 1.1.1.4 Reprenons les exemples précédents.

- La loi $+$ sur $\mathbb{N}$ est associative, commutative et admet 0 pour élément neutre.
- La loi $\times$ sur $\mathbb{C}$ est associative, commutative et admet 1 pour neutre.
- La loi $\cup$ est associative, commutative et admet $\emptyset$ pour neutre.
- La loi $\wedge$ n'est ni associative, ni commutative et n'admet pas d'élément neutre. En effet,
  - on a, par exemple, $\vec{i} \wedge (\vec{i} \wedge \vec{j}) = \vec{i} \wedge \vec{k} = -\vec{j}$ alors que $(\vec{i} \wedge \vec{i}) \wedge \vec{k} = \vec{0}$. Par conséquent, il existe trois vecteurs de l'espace tels que : $\vec{i} \wedge (\vec{i} \wedge \vec{j}) \neq (\vec{i} \wedge \vec{j}) \wedge \vec{k}$. Ceci prouve que $\wedge$ n'est pas associative.
  - Si $\vec{u}$ et $\vec{v}$ sont non colinéaires, $\vec{v} \wedge \vec{u} = -\vec{u} \wedge \vec{v}$ et $\vec{u} \wedge \vec{v} \neq \vec{0}$ donc $\vec{u} \wedge \vec{v} \neq \vec{v} \wedge \vec{u}$. Par suite, $\wedge$ n'est pas commutative.
  - Enfin, s'il existait un élément neutre $\vec{e}$, on aurait : $\vec{e} = \vec{e} \wedge \vec{e} = \vec{0}$. Mais alors, si $\vec{u}$ est un vecteur non nul, $\vec{u} \wedge \vec{e} = \vec{0} \neq \vec{u}$.

  On peut remarquer que dans la pratique, ceci signifie que les règles de calcul de produit vectoriel sont « plus difficiles » que les règles de calcul dans $\mathbb{R}$ par exemple. Pour s'en convaincre, il suffit d'écrire la formule du « double produit vectoriel » et de comparer avec le « double produit » dans $\mathbb{R}$:

  $$\forall (x,y,z) \in \mathbb{R}^3 \text{ , } (x \times y) \times z = x \times (y \times z) = x \times y \times z$$

  alors que pour $\vec{u}, \vec{v}, \vec{w}$ trois vecteurs de l'espace :

  $$(\vec{u} \wedge \vec{v}) \wedge \vec{w} = (\vec{u} \cdot \vec{w})\vec{v} - (\vec{v} \cdot \vec{w})\vec{u}$$

  Formule nettement plus « difficile », ne serait-ce qu'à retenir.
- Si E est un ensemble, la loi $\circ$ sur $\mathcal{F}(E,E)$ est associative, admet un élément neutre (Id_E) mais n'est pas commutative (si E contient au moins deux éléments).

Dans toute la suite, sauf mention explicite du contraire, E est un ensemble quelconque non vide.

Proposition 1.1.1.5 *Soit $\star$ une loi de composition interne sur E. Si $\star$ admet un élément neutre, alors il est unique.*

Preuve :

Soient $e \in E$ et $e' \in E$ deux éléments neutres pour $\star$. Alors :

$$\begin{array}{rcll} e & = & e \star e' & \text{(puisque } e' \text{ est un élément neutre pour } \star) \\ & = & e' & \text{(puisque } e \text{ est un élément neutre pour } \star) \end{array}$$

⊠

Définition 1.1.1.6 Soit $\star$ une loi de composition interne sur E admettant un élément neutre e. Soit x un élément de E. On dit que x est inversible pour la loi $\star$ s'il existe $y \in E$ tel que : $x \star y = y \star x = e$. Un tel y est alors appelé un inverse de x.

⚠ **Attention :** il faut bien vérifier les deux égalités ! Il se peut qu'il existe $y \in E$ tel que $x \star y = e$ mais que $y \star x \neq e$.
Par exemple, si $E = \mathcal{F}(\mathbb{N}, \mathbb{N})$ est muni de la loi $\circ$, on a vu que $\mathrm{Id}_{\mathbb{N}}$ est l'élément neutre et si on considère les applications f et g définies par :

$$\forall n \in \mathbb{N}\ ,\ f(n) = n+1 \quad ; \quad g(0) = 0 \text{ et } \forall n \in \mathbb{N}^\star\ ,\ g(n) = n-1$$

Alors $g \circ f = \mathrm{Id}_{\mathbb{N}}$ mais $f \circ g \neq \mathrm{Id}_{\mathbb{N}}$.

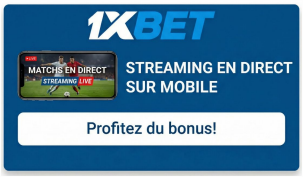
Proposition 1.1.1.7 *Soit $\star$ une loi de composition interne sur E, associative et possédant un neutre. Si $x \in E$ est inversible, alors son inverse est unique.*
Son inverse est alors noté x^{-1}.

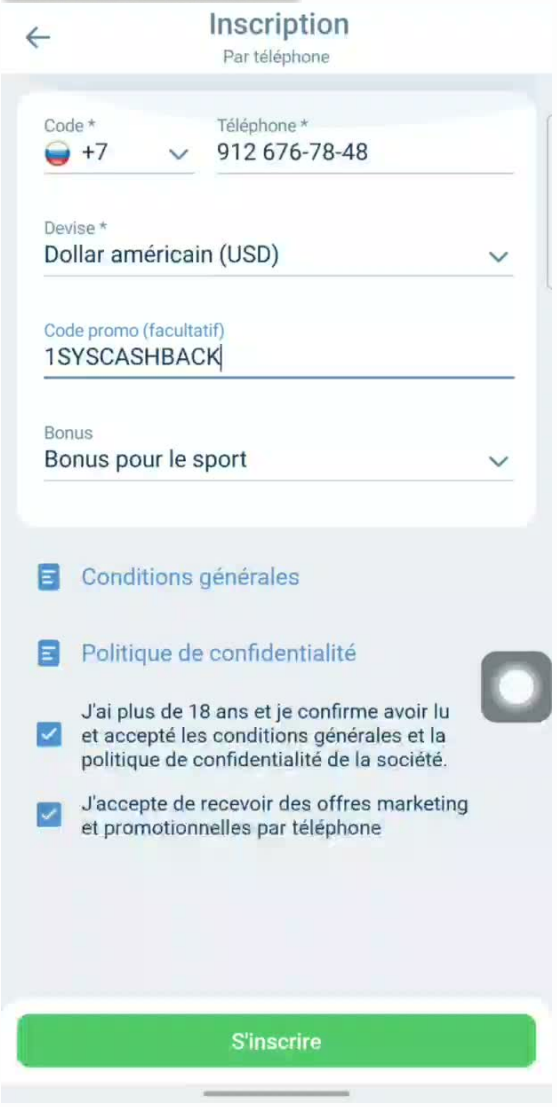
Preuve :

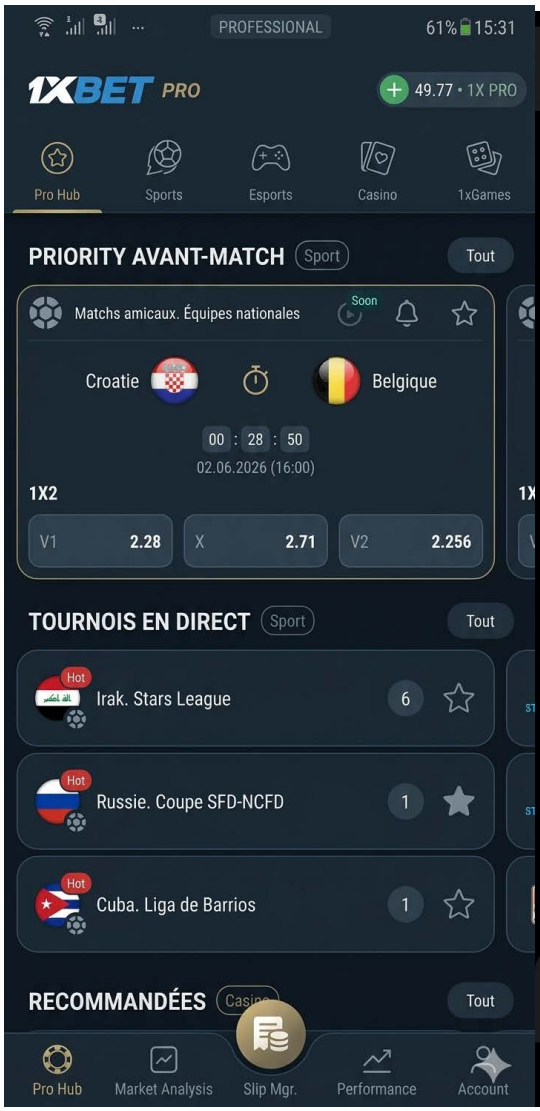
En effet, si $y \in E$ et $y' \in E$ sont deux inverses de x, alors :

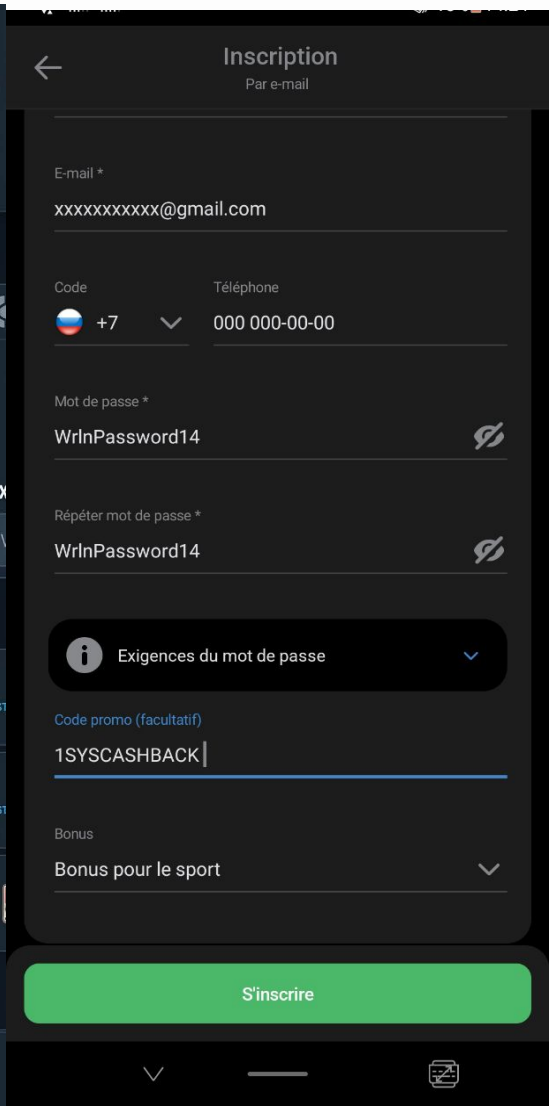
$$y = y \star e = y \star (x \star y') = (y \star x) \star y' = e \star y' = y'$$

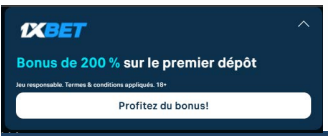
⊠

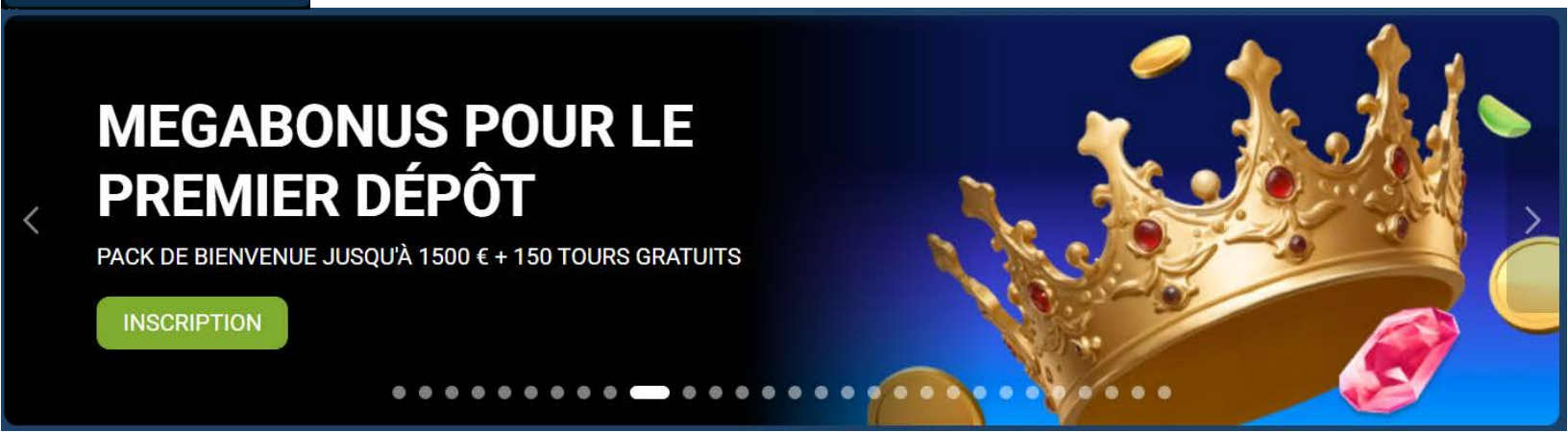

1XBET
STREAMING EN DIRECT SUR MOBILE
Profitez du bonus!


Inscription
Par téléphone
Code *
+7
Téléphone *
912 676-78-48
Devise *
Dollar américain (USD)
Code promo (facultatif)
1SYSCASHBACK
Bonus
Bonus pour le sport
Conditions générales
Politique de confidentialité
J'ai plus de 18 ans et je confirme avoir lu et accepté les conditions générales et la politique de confidentialité de la société.
J'accepte de recevoir des offres marketing et promotionnelles par téléphone
S'inscrire


PROFESSIONAL
61% 15:31
1XBET PRO
49.77 • 1X PRO
Pro Hub
Sports
Esports
Casino
1xGames
PRIORITY AVANT-MATCH
Sport
Tout
Matchs amicaux. Équipes nationales
Soon
Croatie
Belgique
00 : 28 : 50
02.06.2026 (16:00)
1X2
V1 2.28
X 2.71
V2 2.256
TOURNOIS EN DIRECT
Sport
Tout
Hot
Irak. Stars League
6
Russie. Coupe SFD-NCFD
1
Cuba. Liga de Barrios
1
RECOMMANDÉES
Casino
Tout
Pro Hub
Market Analysis
Slip Mgr.
Performance
Account


Inscription
Par e-mail
E-mail *
xxxxxxxxxx@gmail.com
Code
+7
Téléphone
000 000-00-00
Mot de passe *
WrlnPassword14
Répéter mot de passe *
WrlnPassword14
Exigences du mot de passe
Code promo (facultatif)
1SYSCASHBACK
Bonus
Bonus pour le sport
S'inscrire


1XBET
Bonus de 200 % sur le premier dépôt
Jeu responsable. Termes & conditions appliqués. 18+
Profitez du bonus!


MEGABONUS POUR LE PREMIER DÉPÔT
PACK DE BIENVENUE JUSQU'À 1500 € + 150 TOURS GRATUITS
INSCRIPTION

Remarque : *on peut plus généralement définir les notions d'élément inversible à droite, d'élément inversible à gauche, d'inverse à droite et d'inverse à gauche de la façon suivante :*

- *on dit que $x \in E$ est inversible à gauche s'il existe $y \in E$ tel que $y \star x = e$. Un tel élément $y \in E$ est alors appelé un inverse à gauche de x ;*
- *on dit que $x \in E$ est inversible à droite s'il existe $z \in E$ tel que $x \star z = e$. Un tel élément $y \in E$ est alors appelé un inverse à droite de x.*

En revanche, si x est inversible à gauche mais n'est pas inversible, un inverse à gauche n'est pas nécessairement unique. Par exemple, si $E = \mathcal{F}(\mathbb{N}, \mathbb{N})$ est muni de la loi $\circ$ et si $f : \begin{array}{ccc} \mathbb{N} & \longrightarrow & \mathbb{N} \\ n & \longmapsto & n+1 \end{array}$, alors pour tout $a \in \mathbb{N}$, l'application g_a définie par $g_a(0) = a$ et $\forall n \in \mathbb{N}^\star$, $g_a(n) = n-1$, vérifie $g_a \circ f = Id_{\mathbb{N}}$ et par suite, f admet une infinité d'inverses à gauche.

Exercice 1.1.1.8 Montrer que si $\star$ est associative et admet un neutre, et si x admet un inverse à gauche et à droite, alors les inverses à gauche et à droite sont égaux.

Exercice 1.1.1.9 Soit $E = \mathcal{F}(\mathbb{N}, \mathbb{N})$ muni de la loi de composition interne $\circ$. Quels sont les éléments qui sont inversibles à droite ?

Proposition 1.1.1.10 *Soit $\star$ associative et possédant un neutre e. Soient x et y deux éléments inversibles pour la loi $\star$. Alors :*

(i) x^{-1} est inversible et $(x^{-1})^{-1} = x$;

(ii) $x \star y$ est aussi inversible et $(x \star y)^{-1} = y^{-1} \star x^{-1}$.

Preuve :

(i) Par définition, $x \star x^{-1} = x^{-1} \star x = e$. Par suite, x^{-1} est inversible et son inverse est x, c'est-à-dire $(x^{-1})^{-1} = x$.

(ii) On fait le calcul :

$$\begin{array}{rcll} (x \star y) \star (y^{-1} \star x^{-1}) & = & x \star (y \star y^{-1}) \star x^{-1} & (\text{car } \star \text{ est associative}) \\ & = & x \star e \star x^{-1} & \\ & = & x \star x^{-1} & (e \text{ est neutre pour } \star) \\ & = & \text{e} & \end{array}$$

On montre de la même façon que $(y^{-1} \star x^{-1}) \star (x \star y) = e$.
Par conséquent, $x \star y$ est inversible et : $(x \star y)^{-1} = y^{-1} \star x^{-1}$.

$\boxtimes$

⚠ **Attention :** remarquez l'inversion de l'ordre ! Il faut donc faire très attention lorsqu'on travaille avec des lois non commutatives.

Exemple 1.1.1.11 Soient f et g deux bijections de E dans E. Alors $g \circ f$ est bijective et $(g \circ f)^{-1} = f^{-1} \circ g^{-1}$.

Remarques et notations : *soit $\star$ une loi associative et possédant un neutre.*

• *Si la loi de composition interne $\star$ est également commutative, on la note souvent $+$; le neutre est alors noté 0_E (ou bien 0 s'il n'y a pas de risque de confusion) et l'inverse de x est noté $-x$ et on l'appelle aussi l'opposé de x. On dit alors qu'on utilise la notation additive pour $\star$.*

• *On la note aussi souvent $\cdot$ ou $\times$ (notation multiplicative) ; le neutre est alors noté 1_E (ou bien 1 s'il n'y a pas de risque de confusion) et l'inverse de x est encore noté x^{-1}.*

• *Avec l'hypothèse d'associativité, on peut définir sans ambiguïté :*

$$\sum_{i=1}^{n} x_i := x_1 + x_2 + \cdots + x_n \qquad \text{(si } \star \text{ est notée additivement)}$$
$$\prod_{i=1}^{n} x_i := x_1 \star x_2 \star \cdots \star x_n \qquad \text{(si } \star \text{ est notée multiplicativement)}$$

L'associativité fait que ces deux éléments sont bien définis. En revanche, il faut faire attention à l'ordre ! Si la loi $\star$ n'est pas commutative, on peut avoir :

$$\prod_{i=1}^{n} x_i \neq \prod_{i=1}^{n} x_{n-i} \quad \text{(par exemple)}$$

En particulier, en notation multiplicative, on note pour $n \in \mathbb{Z}$:

$$x^n = \prod_{i=1}^{n} x = \underbrace{x \star x \star \cdots \star x}_{n \text{ facteurs}} \text{ si } n \in \mathbb{N}^\star \quad ; \quad x^0 = e$$

et

$$x^n = \prod_{i=1}^{|n|} x^{-1} = \underbrace{x^{-1} \star x^{-1} \star \cdots \star x^{-1}}_{|n| \text{ facteurs}} \text{ si } n < 0$$

De façon similaire, si la loi de composition interne est notée additivement, on pose $nx = 0$ si $n = 0_{\mathbb{Z}}$ et :

$$nx = \sum_{i=1}^{n} x = \underbrace{x + x + \cdots + x}_{n \text{ termes}} \text{ si } n > 0$$

et

$$nx = \sum_{i=1}^{|n|}(-x) = \underbrace{(-x)+(-x)+\cdots+(-x)}_{|n| \text{ termes}} \text{ si } n<0$$

Je vous laisse alors vérifier en exercice que les règles de calculs usuelles sont encore valables, c'est-à-dire :

$$\forall (n,p)\in\mathbb{Z}^2 \ , \ x^{n+p} = x^n \star x^p \quad \textit{(en notation multiplicative)}$$

$$\forall (n,p)\in\mathbb{Z}^2 \ , \ (n+p)x = nx+px \quad \textit{(en notation additive)}$$

1.1.2 Définition d'un groupe et règles de calcul

Définition 1.1.2.1 Soient G un ensemble et $\star$ une loi de composition interne sur G. On dit que $(G,\star)$ est un groupe s'il vérifie les trois propriétés suivantes :

(i) $\star$ est associative ;

(ii) $\star$ possède un neutre ;

(iii) tout élément de G est inversible pour la loi $\star$.

Si de plus, $\star$ est commutative, on dit que $(G,\star)$ est un groupe abélien (ou commutatif).

Proposition 1.1.2.2 *Les ensembles suivants, munis des lois de composition interne données sont des groupes (de référence) :*

$$(\mathbb{Z},+) \ ; \ (\mathbb{Q},+) \ ; \ (\mathbb{R},+) \ ; \ (\mathbb{C},+) \ ; \ (\mathbb{Q}^\star,\times) \ ; \ (\mathbb{R}^\star,\times) \ ; \ (\mathbb{C}^\star,\times)$$

De plus, ce sont tous des groupes commutatifs.

Preuve :

C'est clair compte-tenu des propriétés de l'addition et de la multiplication dans $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ et $\mathbb{C}$.

⊠

Remarque : *un groupe n'est jamais un ensemble vide puisque par définition, il existe un élément neutre dans G.*

Exercice 1.1.2.3 En revanche, $(\mathbb{N}, +)$ et $(\mathbb{C}, \times)$ ne sont pas des groupes. Pourquoi ?

Exercice 1.1.2.4 Montrer que $(\mathbb{U}, \times)$ est un groupe commutatif. *On rappelle que l'ensemble* $\mathbb{U}$ *est défini par* $\mathbb{U} = \{z \in \mathbb{C} \ / \ |z| = 1\}$.

Proposition 1.1.2.5 *Soient* $\mathbb{K} \in \{\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}\}$ *et* $n \in \mathbb{N}^\star$. *On définit l'application* $+$ *de* $\mathbb{K}^n \times \mathbb{K}^n$ *dans* $\mathbb{K}^n$ *par :*

$$\forall ((x_i)_{1\leqslant i\leqslant n}, (y_i)_{1\leqslant i\leqslant n}) \in \mathbb{K}^n \times \mathbb{K}^n \ , \ (x_i)_{1\leqslant i\leqslant n} + (y_i)_{1\leqslant i\leqslant n} := (x_i + y_i)_{1\leqslant i\leqslant n}$$

Alors $(\mathbb{K}^n, +)$ *est un groupe commutatif : c'est un groupe de référence.*

Remarque : *attention, dans la proposition, il y a bien deux opérations « + » différentes ! La première est celle que l'on définit (c'est-à-dire l'opération sur l'ensemble* $\mathbb{K}^n$*) et l'autre est l'addition usuelle dans* $\mathbb{K}$ *! S'il y a un risque de confusion, on peut aussi noter l'addition dans* $\mathbb{K}$ *en utilisant la notation* $+_{\mathbb{K}}$.

Preuve :

• Pour commencer, on peut remarquer que $+ : \mathbb{K}^n \times \mathbb{K}^n \longrightarrow \mathbb{K}^n$ est une application bien définie (car $+_{\mathbb{K}}$ est bien une loi de composition interne sur $\mathbb{K}$).

• Puisque l'addition dans $\mathbb{K}$ est commutative, il est clair que $+$ est commutative.

• Notons $0_{\mathbb{K}^n} = \underbrace{(0_{\mathbb{K}}, \cdots, 0_{\mathbb{K}})}_{n \text{ termes}} = (0_{\mathbb{K}})_{1\leqslant i\leqslant n}$. Alors $0_{\mathbb{K}^n} \in \mathbb{K}^n$ et pour tout $x = (x_i)_{1\leqslant i\leqslant n} \in \mathbb{K}^n$:

$$x + 0_{\mathbb{K}^n} = (x_i +_{\mathbb{K}} 0_{\mathbb{K}})_{1\leqslant i\leqslant n} = (x_i)_{1\leqslant i\leqslant n} = x$$

et puisque $+$ est commutative, $0_{\mathbb{K}^n} + x = x + 0_{\mathbb{K}^n} = x$. Ce qui montre que $+$ admet un élément neutre : l'élément $0_{\mathbb{K}^n}$.

• L'associativité de $+$ est une conséquence immédiate de l'associativité de l'addition dans $\mathbb{K}$. En effet, soient $x = (x_i)_{1\leqslant i\leqslant n}$, $y = (y_i)_{1\leqslant i\leqslant n}$ et $z = (z_i)_{1\leqslant i\leqslant n}$ trois éléments de $\mathbb{K}^n$. Alors :

$$\begin{aligned}(x + y) + z &= (x_i +_{\mathbb{K}} y_i)_{1\leqslant i\leqslant n} + (z_i)_{1\leqslant i\leqslant n} \\ &= ((x_i +_{\mathbb{K}} y_i) +_{\mathbb{K}} z_i)_{1\leqslant i\leqslant n} \\ &= (x_i +_{\mathbb{K}} (y_i +_{\mathbb{K}} z_i))_{1\leqslant i\leqslant n} \\ &= (x_i)_{1\leqslant i\leqslant n} + (y_i +_{\mathbb{K}} z_i)_{1\leqslant i\leqslant n}\end{aligned}$$

Ainsi,

$$\begin{aligned}(x+y)+z &= (x_i)_{1\leqslant i\leqslant n} + (y_i +_{\mathbb{K}} z_i)_{1\leqslant i\leqslant n}\\ &= x+(y+z)\end{aligned}$$

prouvant ainsi que $+$ est associative.

• Enfin, montrons que tout élément de $\mathbb{K}^n$ est inversible pour $+$.
Soit $x=(x_i)_{1\leqslant i\leqslant n}\in\mathbb{K}^n$. Posons $y=(-x_i)_{1\leqslant i\leqslant n}$. Alors $y\in\mathbb{K}^n$ et :

$$\begin{aligned}x+y &= (x_i +_{\mathbb{K}} (-x_i))_{1\leqslant i\leqslant n}\\ &= (0_{\mathbb{K}})_{1\leqslant i\leqslant n}\\ &= 0_{\mathbb{K}^n}\end{aligned}$$

Or, $+$ est commutative donc $0_{\mathbb{K}^n}=x+y=y+x$. Ce qui prouve que x est inversible (et que y est son inverse).

On a donc démontré que $(\mathbb{K}^n,+)$ est un groupe commutatif.

⊠

Remarques et notations :

- *dans la pratique, on n'écrit pas $+_{\mathbb{K}}$. On utilise le même symbole $+$ pour désigner les deux opérations différentes. C'est à vous de bien réfléchir à chaque fois pour comprendre de quelle opération on parle : s'agit-il d'une addition de nombres (c'est-à-dire dans $\mathbb{K}$) ou d'une addition de « vecteurs » (c'est-à-dire dans $\mathbb{K}^n$) ?*
- *Si cette écriture formelle vous dérange, on peut aussi reformuler dans le cas particulier $\mathbb{K}=\mathbb{R}$ et $n=2$. L'opération $+$ dans $\mathbb{R}^2$ est définie par :*

$$\forall((x,y),(x',y'))\in\mathbb{R}^2\times\mathbb{R}^2\ ,\ (x,y)+(x',y')=(x+x',y+y')$$

Il s'agit bien de l'addition usuelle de vecteurs de $\mathbb{R}^2$. Le neutre est $(0_{\mathbb{R}},0_{\mathbb{R}})=(0,0)$ (le vecteur nul de $\mathbb{R}^2$) et pour $(x,y)\in\mathbb{R}^2$, l'inverse de (x,y) pour la loi $+$ est $(-x,-y)$ (le vecteur opposé usuel dans $\mathbb{R}^2$).

Proposition 1.1.2.6 *Soient X un ensemble non vide quelconque et $\mathbb{K}\in\{\mathbb{Z},\mathbb{Q},\mathbb{R},\mathbb{C}\}$. On définit l'application, notée $+$, de $\mathcal{F}(X,\mathbb{K})\times\mathcal{F}(X,\mathbb{K})$ dans $\mathcal{F}(X,\mathbb{K})$ par :*

$$\forall(f,g)\in\mathcal{F}(X,\mathbb{K})^2\ ,\ f+g:=\begin{array}{ccc}X&\longrightarrow&\mathbb{K}\\ x&\longmapsto&f(x)+g(x)\end{array}$$

Alors, $(\mathcal{F}(X,\mathbb{K}),+)$ est un groupe commutatif : c'est un groupe de référence.

Preuve :

Laissée en exercice (voir la preuve de la proposition 3.2.1.3).

⊠

Proposition 1.1.2.7 *Soit E un ensemble. On note $\sigma(E)$ l'ensemble des bijections de E dans E. Alors $(\sigma(E), \circ)$ est un groupe, appelé groupe des permutations de E. De plus, il est non abélien (dès que E contient au moins trois éléments).*

Preuve :

Montrons pour commencer que $(\sigma(E), \circ)$ est un groupe.

• On sait déjà que la composée de deux bijections est encore une bijection. Par suite, $\circ$ est bien une loi de composition interne sur $\sigma(E)$.

• On a prouvé, dans le cours sur les applications, que la loi $\circ$ est associative (lorsqu'elle est définie, ce qui est le cas ici).

• L'application Id_E appartient à $\sigma(E)$ et clairement :

$$\forall f \in \sigma(E)\ ,\ f \circ \mathrm{Id}_E = \mathrm{Id}_E \circ f = f$$

Par suite, Id_E est l'élément neutre de $\sigma(E)$ pour la loi $\circ$.

• Enfin, soit $f \in \sigma(E)$. Par définition, f est bijective : elle admet donc une bijection réciproque g, qui est elle aussi une bijection de E dans E, c'est-à-dire $g \in \sigma(E)$. De plus, g vérifie :

$$f \circ g = g \circ f = \mathrm{Id}_E$$

Par conséquent, tout élément $f \in \sigma(E)$ admet un inverse (dans $\sigma(E)$) pour la loi $\circ$.

Ceci prouve que $(\sigma(E), \circ)$ est un groupe.

Montrons à présent que si E contient au moins trois éléments, ce groupe n'est pas commutatif. Soient x_1, x_2, x_3 trois éléments distincts de E et considérons les deux applications suivantes :

$$\tau : E \longrightarrow E,\quad x \longmapsto \begin{cases} x_2 & \text{si } x = x_1 \\ x_1 & \text{si } x = x_2 \\ x & \text{sinon} \end{cases} \qquad \text{et} \qquad \tau' : E \longrightarrow E,\quad x \longmapsto \begin{cases} x_3 & \text{si } x = x_1 \\ x_1 & \text{si } x = x_3 \\ x & \text{sinon} \end{cases}$$

Il est clair que $\tau^2 = \tau'^2 = \mathrm{Id}_E$. Par conséquent, $\tau, \tau' \in \sigma(E)$ et de plus :

$$(\tau \circ \tau')(x_1) = x_3 \quad \text{et} \quad (\tau' \circ \tau)(x_1) = x_2$$

Par suite, $\tau \circ \tau' \neq \tau' \circ \tau$, prouvant ainsi que $(\sigma(E), \circ)$ n'est pas un groupe commutatif.

$\boxtimes$

Définition 1.1.2.8 Pour $n \in \mathbb{N}^\star$, l'ensemble des bijections de $[\![1, n]\!]$ dans lui-même est un groupe pour la loi $\circ$. Ce groupe est appelé groupe symétrique (d'ordre n) et on le note S_n.

Remarques : *on peut noter les points suivants :*

- $(S_n, \circ)$ *est bien un groupe d'après la proposition précédente ;*
- S_n *est un groupe fini (c'est-à-dire un groupe et un ensemble fini) de cardinal* $n!$ *;*
- *c'est un groupe de référence qui est très important. On l'étudiera de façon plus précise dans le cours sur les déterminants (cours de mathématiques spéciales 1).*

Proposition 1.1.2.9 *Soient $(G, \star)$ un groupe et $a, b \in G$. Les équations $a \star x = b$ et $y \star a = b$ admettent chacune une unique solution qui sont respectivement $x = a^{-1} \star b$ et $y = b \star a^{-1}$. Autrement dit, les applications :*

$$\begin{array}{ccc} G & \xrightarrow{\gamma_a} & G \\ x & \longmapsto & a \star x \end{array} \quad et \quad \begin{array}{ccc} G & \xrightarrow{\delta_a} & G \\ y & \longmapsto & y \star a \end{array}$$

sont des applications bijectives.

Preuve :

Montrons par exemple que γ_a est bijective.

• γ_a est une application bien définie car $\star$ est une loi de composition interne sur G.

• Montrons que γ_a est injective.
Soit $(x, y) \in G^2$ tel que $\gamma_a(x) = \gamma_a(y)$, c'est-à-dire $a \star x = a \star y$. Alors en multipliant à gauche par a^{-1} (l'inverse de a dans G, qui existe puisque G est un groupe), on a :

$$a^{-1} \star (a \star x) = a^{-1} \star (a \star y) \text{ c'est-à-dire } (a^{-1} \star a) \star x = (a^{-1} \star a) \star y$$

car $\star$ est associative. Enfin, par définition, en notant $e \in G$ l'élément neutre pour $\star$, on a donc $e \star x = e \star y$, c'est-à-dire $x = y$.

Ce qui prouve que γ_a est injective.

• Montrons enfin que γ_a est surjective.
Soit $y \in G$. Posons $x = a^{-1} \star y$: alors $x \in G$ et $\gamma_a(x) = y$.

Ce qui prouve que γ_a est surjective.

⊠

Remarques :

- *pour prouver que γ_a est bijective, on pouvait aussi fixer $y \in G$ et montrer que l'équation $\gamma_a(x) = y$ admet une unique solution par analyse-synthèse (l'analyse prouvant l'injectivité et la synthèse la surjectivité) ;*
- *on pouvait également montrer directement que $\gamma_a^{-1} = \gamma_{a^{-1}}$ et $\delta_a^{-1} = \delta_{a^{-1}}$;*
- *enfin, on retient que l'injectivité signifie que dans un groupe, on peut « simplifier » par a des deux côtés d'une égalité (« simplifier » signifie mathématiquement multiplier par l'inverse de l'élément), à condition que le facteur soit du « même côté » :*

$$\forall (x, y) \in G^2 \ , \ (a \star x = a \star y \iff x = y)$$

1.1.3 Sous-groupes

Définition 1.1.3.1 Soient $(G, \star)$ un groupe de neutre e et H une partie de G. On dit que H est un sous-groupe de G si H vérifie les trois propriétés suivantes :

(i) $e \in H$;

(ii) H est stable par $\star$: $\forall (x, y) \in H^2 \ , \ x \star y \in H$;

(iii) H est stable par inverse : $\forall x \in H \ , \ x^{-1} \in H$.

Remarques importantes :

- *en fait, on peut remplacer (i) par $(i)'$: H est non vide. Les propriétés (ii) et (iii) permettent alors de prouver que $e \in H$;*
- *les propriétés (ii) et (iii) sont équivalentes à $(ii)'$: $\forall (x, y) \in H^2 \ , \ x \star y^{-1} \in H$;*
- *en pratique, la plupart du temps, pour prouver que H est un sous-groupe de G, on prouvera que $e \in H$ et que $(ii)'$ est vérifiée ;*
- *si H est un sous-groupe de $(G, \star)$, alors $(H, \star)$ est un groupe.*

Exemple 1.1.3.2 $(\mathbb{Z}, +)$ est un sous-groupe de $(\mathbb{Q}, +)$ qui est lui-même un sous-groupe de $(\mathbb{R}, +)$.

Exemple 1.1.3.3 $(\mathbb{U}, \times)$ est un sous-groupe de $(\mathbb{C}^\star, \times)$. En effet,

- $\mathbb{U} \subset \mathbb{C}^\star$ (par définition) ;
- $|1| = 1$ donc $1_{\mathbb{C}} \in \mathbb{U}$ (on note ici $1_{\mathbb{C}}$ le nombre complexe 1) ;
- et enfin, pour tout $(z, z') \in \mathbb{U}^2$, on a :

$$|z^{-1} \times z'| = |z|^{-1} \times |z'| = 1^{-1} \times 1 = 1 \text{ donc } z^{-1} \times z' \in \mathbb{U}$$

▶ Méthode :

Dans la pratique, pour montrer qu'un ensemble donné est un groupe, on montre presque toujours que c'est un sous-groupe d'un groupe connu.
Il est donc important de bien connaître les groupes de référence !

Exemple 1.1.3.4 Montrons que $(\mathbb{R}^{+\star}, \times)$ est un groupe mais que $(\mathbb{R}^{\star -}, \times)$ ne l'est pas.

• Montrons que $(\mathbb{R}^{+\star}, \times)$ est un sous-groupe de $(\mathbb{R}^\star, \times)$.

∗ Montrons que $\mathbb{R}^{+\star}$ contient le neutre de $\mathbb{R}^\star$ pour la loi $\times$.

De façon évidente, $1_{\mathbb{R}} > 0$ donc $1 \in \mathbb{R}^{+\star}$.

∗ Montrons que $\mathbb{R}^{+\star}$ est stable par $\times$.

Il est clair que : $\forall x, y \in \mathbb{R}^{+\star}$, $x \times y \in \mathbb{R}^{+\star}$.

∗ Enfin, montrons que $\mathbb{R}^{+\star}$ est stable par inverse.

Il est clair que : $\forall x > 0$, $x^{-1} = \dfrac{1}{x} > 0$. Par conséquent, si $x \in \mathbb{R}^{+\star}$, alors $x^{-1} \in \mathbb{R}^{+\star}$.

Ceci prouve que $\mathbb{R}^{+\star}$ est un sous-groupe de $(\mathbb{R}^\star, \times)$. Par conséquent, $(\mathbb{R}^{+\star}, \times)$ est un groupe.

• En revanche, $\times$ n'est pas une loi de composition interne sur $\mathbb{R}^{-\star}$ puisque par exemple, $-1 \in \mathbb{R}^{-\star}$ mais $(-1) \times (-1) = 1 > 0$, c'est-à-dire $(-1) \times (-1) \notin \mathbb{R}^{-\star}$.

Exemple 1.1.3.5 On montrera dans le chapitre sur les suites que l'ensemble des suites convergentes est un sous-groupe de $(\mathbb{R}^{\mathbb{N}}, +)$.

Exemple 1.1.3.6 L'ensemble $\mathcal{C}^0(\mathbb{R}, \mathbb{R})$ est un sous-groupe de $(\mathcal{F}(\mathbb{R}, \mathbb{R}), +)$.

Exemple 1.1.3.7 L'ensemble $\mathcal{S}_H$ des solutions de $y'' - y = 0$ est un sous-groupe de $(\mathcal{F}(\mathbb{R}, \mathbb{R}), +)$. En effet,

- $\mathcal{S}_H \subset \mathcal{F}(\mathbb{R}, \mathbb{R})$;
- la fonction constante égale à 0, c'est-à-dire le neutre de + dans $\mathcal{F}(\mathbb{R}, \mathbb{R})$, est bien solution de $y'' - y = 0$. Ce qui prouve que $0_{\mathcal{F}(\mathbb{R},\mathbb{R})} \in \mathcal{S}_H$;
- enfin, si $y_1, y_2 \in \mathcal{S}_H$, alors $y_1 - y_2 = y_1 + (-y_2) \in \mathcal{S}_H$ (propriété des solutions d'une équation différentielle linéaire).

Ce qui prouve que $\mathcal{S}_H$ est bien un sous-groupe de $\mathcal{F}(\mathbb{R}, \mathbb{R})$.

Exercice 1.1.3.8 L'ensemble $\mathcal{S}$ des solutions de $y'' - y = 1$ est-il un sous-groupe de $(\mathcal{F}(\mathbb{R}, \mathbb{R}), +)$?

Exercice 1.1.3.9 Soit Ω un univers fini non vide. D'après la proposition précédente (avec $X = \mathcal{P}(\Omega)$), l'ensemble $G = \mathcal{F}(\mathcal{P}(\Omega), \mathbb{R})$ des applications de $\mathcal{P}(\Omega)$ dans $\mathbb{R}$ est un groupe pour l'addition.

1. L'ensemble des variables aléatoires réelles sur Ω est-il un sous-groupe de G ?
2. L'ensemble des applications $P \in G$ vérifiant :

$$\forall (A, B) \in \mathcal{P}(\Omega)^2 \ , \ P(A \sqcup B) = P(A) + P(B)$$

   est-il un sous-groupe de G ?
3. L'ensemble des mesures de probabilités sur $\mathcal{P}(\Omega)$ est-il un sous-groupe de G ?

1.1.4 Opérations sur les sous-groupes

Dans ce paragraphe, on fixe un groupe $(G, \star)$ et on va s'intéresser aux opérations (ensemblistes) que l'on peut faire avec les sous-groupes. Mais avant de traiter le cas général, on va commencer par un exercice.

Exercice 1.1.4.1 On considère ici $G = \mathbb{R}^2$ muni de l'addition usuelle ainsi que les ensembles $H = \{(x, 0) \ , \ x \in \mathbb{R}\}$ et $K = \{(0, y) \ , \ y \in \mathbb{R}\}$.

1. Montrer que H et K sont des sous-groupes de G.
2. $\overline{H} = G \setminus H$ est-il un sous-groupe de G ?
3. $H \cup K$ est-il un sous-groupe de G ?
4. $H \cap K$ est-il un sous-groupe de G ?

Plus généralement, on dispose des propriétés suivantes sur les sous-groupes.

Proposition 1.1.4.2 *Soient G un groupe et H, K deux sous-groupes de G. Alors $H \cap K$ est un sous-groupe de G.*

Preuve :

Montrons que $H \cap K$ est un sous-groupe de G.

• Montrons que le neutre e de G appartient à $H \cap K$.

On sait que H et K sont des sous-groupes de G. Par définition d'un sous-groupe, $e \in H$ et $e \in K$. Par suite, $e \in H \cap K$.

• Montrons que $H \cap K$ est stable par $\star$.

Soient x et y deux éléments de $H \cap K$. H étant un sous-groupe de G, $x \star y \in H$. De la même façon, K étant aussi un sous-groupe de G, $x \star y \in K$. Par suite, $x \star y \in H \cap K$ prouvant que $H \cap K$ est stable par $\star$.

• Montrons que $H \cap K$ est stable par inverse.

Soit $x \in H \cap K$. H et K étant des sous-groupes de G, ils sont stables par inverse. Par suite, $x^{-1} \in H$ et $x^{-1} \in K$, c'est-à-dire $x^{-1} \in H \cap K$.

Ce qui prouve que $H \cap K$ est un sous-groupe de G.

⊠

⚠ **Attention :** en revanche, attention ! !

- $H \cup K$ n'est pas forcément un sous-groupe ! ! ! On verra en exercice que :

$$H \cup K \text{ est un sous-groupe de } G \iff (H \subset K \text{ ou } K \subset H)$$

- $\overline{H} = G \setminus H$ n'est jamais un sous-groupe de G !

En fait, la proposition précédente peut se généraliser à une intersection quelconque (la démonstration est identique et laissée en exercice).

Proposition 1.1.4.3 *Soit G un groupe et soit $(H_i)_{i \in I}$ une famille quelconque (c'est-à-dire finie ou infinie) de sous-groupes de G. Alors, $\bigcap_{i \in I} H_i$ est un sous-groupe de G.*

1.1.5 Morphismes de groupes

Définition 1.1.5.1 Soient $(G, \star)$ et $(H, \diamond)$ deux groupes. On dit qu'une application $f : G \longrightarrow H$ est un morphisme de groupes si elle « préserve les opérations des groupes », c'est-à-dire si :

$$\forall (x, y) \in G^2 \ , \ f(x \star y) = f(x) \diamond f(y)$$

Exemple 1.1.5.2 La fonction exponentielle est un morphisme de $(\mathbb{R}, +)$ dans $(\mathbb{R}^\star, \times)$. En effet,

$$\forall x, y \in \mathbb{R} \ , \ \exp(x + y) = \exp(x) \times \exp(y)$$

Exemple 1.1.5.3 L'application $\theta \longmapsto e^{i\theta}$ est un morphisme de $(\mathbb{R}, +)$ dans $(\mathbb{U}, \times)$.

Exercice 1.1.5.4 En revanche, γ_a et δ_a ne sont pas des morphismes (sauf si $a = e$).

Exercice 1.1.5.5 Montrer que l'application D, qui à une fonction f de classe $\mathcal{C}^1$ sur $\mathbb{R}$ associe $D(f) = f'$, est un morphisme de $(\mathcal{C}^1(\mathbb{R}, \mathbb{R}), +)$ dans $(\mathcal{C}^0(\mathbb{R}, \mathbb{R}), +)$.

Exercice 1.1.5.6 th est-elle un morphisme de groupes de $(\mathbb{R}, +)$ dans $(\mathbb{R}, +)$?

Exercice 1.1.5.7 L'application $I : \mathcal{C}^0([0, 1]), \mathbb{R}) \longrightarrow \mathbb{R}$ qui à une fonction f continue sur $[0, 1]$ associe $I(f) = \displaystyle\int_0^1 f(x) \, \mathrm{d}x$ est-elle :

1. un morphisme de groupes de $(\mathcal{C}^0(\mathbb{R}, \mathbb{R}), +)$ dans $(\mathbb{R}, +)$?
2. un morphisme de groupes de $(\mathcal{C}^0(\mathbb{R}, \mathbb{R}), \times)$ dans $(\mathbb{R}, \times)$?

Pour la seconde question, on donnera trois raisons distinctes pour lesquelles c'est faux.

Proposition 1.1.5.8 *Soit $G \xrightarrow{f} H$ un morphisme de groupes. Alors :*

(i) $f(1_G) = 1_H$;

(ii) $\forall x \in G \ , \ f(x^{-1}) = f(x)^{-1}$;

(iii) $\forall n \in \mathbb{N}^\star \ , \ \forall x_1, \cdots, x_n \in G \ , \ f(x_1 \star x_2 \star \cdots \star x_n) = f(x_1) \diamond f(x_2) \diamond \cdots \diamond f(x_n)$.

Preuve :

• Montrons (i).

Par définition de l'élément neutre dans un groupe :

$$1_H \diamond f(1_G) = f(1_G) = f(1_G \star 1_G) = f(1_G) \diamond f(1_G)$$

On simplifie à droite par $f(1_G)$ (toujours possible puisque $f(1_G)$ est inversible dans H), ce qui donne : $f(1_G) = 1_H$.

• Montrons (ii).

Soit $x \in G$. f étant un morphisme de groupes, on a :

$$f(x) \diamond f(x^{-1}) = f(x \star x^{-1}) = f(1_G) = 1_H$$

On montre de la même façon que $f(x^{-1}) \diamond f(x) = 1_H$. Par conséquent, $f(x)^{-1} = f(x^{-1})$.

• Enfin, (iii) se montre par récurrence immédiate sur $n \geqslant 1$.

⊠

Proposition 1.1.5.9 (Définition du noyau et de l'image) *Soit $f : G \longrightarrow H$ un morphisme de groupes. On note 1_G (respectivement 1_H) l'élément neutre dans G (respectivement H). On pose :*

$$\mathrm{Im}(f) = f(G) \text{ (image directe de } G)$$

et

$$\ker(f) = f_r^{-1}(\{1_H\}) \text{ (image réciproque de } \{1_H\})$$

(i) $\mathrm{Im}(f)$*, appelé l'image de f, est un sous-groupe de H ;*

(ii) $\ker(f)$*, appelé noyau de f (« kernel »), est un sous-groupe de G ;*

(iii) f est injective si et seulement si $\ker(f) = \{1_G\}$.

Preuve :

Pour commencer, on rappelle les définitions des images directes et réciproques :

$$f(G) = \{y \in H \ / \ \exists x \in G \ , \ y = f(x)\} = \{f(x) \ , \ x \in G\}$$

et

$$\ker(f) = f_r^{-1}(\{1_H\}) = \{x \in G \ / \ f(x) = 1_H\}$$

• (i) Montrons que $\mathrm{Im}(f)$ est un sous-groupe de H.

∗ Tout d'abord, par définition, $\mathrm{Im}(f) \subset H$.

∗ Ensuite, puisque f est un morphisme de groupes, $f(1_G) = 1_H$ et par définition, $f(1_G) \in f(G)$. Par conséquent, $1_H \in f(G)$.

∗ Par ailleurs, soient y et y' deux éléments de $f(G)$. Alors, il existe $x \in G$ et $x' \in G$ tels que $y = f(x)$ et $y' = f(x')$. Alors :

$$y \diamond y' = f(x) \diamond f(x') = f(x \star x')$$

Or, $x \star x' \in G$ donc $f(x \star x') \in f(G)$, c'est-à-dire $y \diamond y' \in f(G)$.

∗ Enfin, soit $y \in f(G)$: il existe $x \in G$ tel que $y = f(x)$. Alors, d'après la proposition 1.1.5.8, $y^{-1} = f(x)^{-1} = f(x^{-1}) \in f(G)$.

Par conséquent, $\mathrm{Im}(f)$ est un sous-groupe de H.

• (ii) Montrons que $\ker(f)$ est un sous-groupe de G.

∗ Par définition d'une image réciproque, $\ker(f) = f_r^{-1}(\{1_H\}) \subset G$.

∗ D'après la proposition précédente, $f(1_G) = 1_H$. Par suite,

$$1_G \in \{x \in G \mid f(x) = 1_H\} = \ker(f)$$

∗ Soient $x, x' \in \ker(f)$. On a alors $f(x) = f(x') = 1_H$ et donc :

$$f(x \star x'^{-1}) = f(x) \diamond f(x'^{-1}) = f(x) \diamond f(x')^{-1} = 1_H \diamond 1_H^{-1} = 1_H$$

Par conséquent, $x \star x'^{-1} \in \ker(f)$.

Ce qui prouve que $\ker(f)$ est un sous-groupe de G.

(iii) Montrons enfin que f est injective si et seulement si $\ker(f) = \{1_G\}$.

∗ Montrons $\Longrightarrow$.

On suppose que f est injective. On montre que $\ker(f) = \{1_G\}$. Pour commencer, on sait que $\{1_G\} \subset \ker(f)$. Montrons alors l'inclusion réciproque. Soit $x \in \ker(f)$. Alors, $f(x) = 1_H = f(1_G)$. f étant injective, $x = 1_G$.
Ce qui prouve que $\ker(f) \subset \{1_G\}$ et donc, par double inclusion, $\ker(f) = \{1_G\}$. D'où la première implication.

∗ Montrons la réciproque.

On suppose que $\ker(f) = \{1_G\}$. Montrons que f est injective. Soient $x, x' \in G$ tels que $f(x) = f(x')$. On a alors :

$$\begin{aligned} f(x) = f(x') &\iff f(x) \diamond f(x')^{-1} = 1_H \\ &\iff f(x \star x'^{-1}) = 1_H \\ &\iff x \star x'^{-1} \in \ker(f) \\ &\iff x \star x'^{-1} = 1_G \\ &\iff x = x' \end{aligned}$$

Ce qui prouve que f est injective.

⊠

Remarque importante : *l'inclusion* $\{1_G\} \subset \ker(f)$ *est toujours vraie pour n'importe quel morphisme de groupes, puisqu'on a montré que* $\ker(f)$ *est un sous-groupe de* G. *Par conséquent, pour montrer que* $\ker(f) = \{1_G\}$, *on ne montre qu'une seule inclusion, à savoir* $\ker(f) \subset \{1_G\}$.

Exemple 1.1.5.10 Reprenons un des exemples précédents. Soit $f : (\mathbb{R}, +) \longrightarrow (\mathbb{C}^\star, \times)$ définie par $f(\theta) = e^{i\theta}$. On a vu que f est un morphisme de groupes.

L'image de f est par définition :

$$\mathrm{Im}(f) = \{z \in \mathbb{C}^\star \mid \exists \theta \in \mathbb{R} \ , \ z = e^{i\theta}\} = \mathbb{U}$$

On en déduit donc directement que $\mathbb{U}$ est un sous-groupe de $(\mathbb{C}^\star, \times)$.

De même, le noyau de f est :

$$\ker(f) = \{\theta \in \mathbb{R} \mid e^{i\theta} = 1\} = \{2k\pi \ , \ k \in \mathbb{Z}\} = 2\pi\mathbb{Z}$$

Ceci permet directement de conclure que l'ensemble $2\pi\mathbb{Z}$ est un sous-groupe de $(\mathbb{R}, +)$.

Exercice 1.1.5.11 Soit $n \in \mathbb{N}^\star$. On considère l'application $\varphi : (\mathbb{Z}, +) \longrightarrow (\mathbb{Z}, +)$ définie par $\varphi(z) = nz$. Montrer que φ est un morphisme de groupes et déterminer son image ainsi que son noyau. Que peut-on en conclure pour l'ensemble $n\mathbb{Z}$?

► Méthode :

Pour montrer que H est un groupe, on peut :

1. montrer que c'est le noyau ou l'image d'un morphisme de groupes ;
2. montrer que c'est un sous-groupe d'un groupe connu ;
3. montrer que c'est une intersection de sous-groupes d'un groupe connu ;
4. revenir à la définition d'un groupe.

Définition 1.1.5.12 (Isomorphisme, endomorphisme et automorphisme)

On dit qu'une application f est :

- un endomorphisme de groupe si f est un morphisme d'un groupe G dans lui-même ;
- un isomorphisme de groupes si f est un morphisme de groupes et si f est bijective ;
- un automorphisme de groupe si f est un isomorphisme d'un groupe G dans lui-même.

Remarque et notations : *un automorphisme est donc un endomorphisme et un isomorphisme. On note Aut(G) l'ensemble des automorphismes de G et End(G) l'ensemble des endomorphismes de G.*

Exemple 1.1.5.13 L'exponentielle $\exp : (\mathbb{R}, +) \longrightarrow (\mathbb{R}^{+\star}, \times)$ est un isomorphisme de groupes mais n'est pas un automorphisme de groupe. En effet,

- on a montré que c'est bien un morphisme de groupes ;
- on sait que la fonction exponentielle est une bijection de $\mathbb{R}$ dans $]0, +\infty[$;
- mais ce n'est pas un automorphisme car $(\mathbb{R}, +)$ et $(\mathbb{R}^{+\star}, \times)$ sont deux groupes différents.

Exemple 1.1.5.14 La conjugaison $c : (\mathbb{C}, +) \longrightarrow (\mathbb{C}, +)$ est un automorphisme de groupe. En effet,

- pour tout $(z, z') \in \mathbb{C}^2$, $c(z + z') = \overline{z + z'} = \overline{z} + \overline{z'} = c(z) + c(z')$, donc c est bien un morphisme de groupes ;
- c est bijective (et $c^{-1} = c$) de $\mathbb{C}$ dans $\mathbb{C}$;
- c est bien une application du groupe $(\mathbb{C}, +)$ dans lui-même.

Exercice 1.1.5.15 Trouver une condition nécessaire et suffisante (sur $n \in \mathbb{N}^{\star}$) pour que l'application φ de l'exercice 1.1.5.11 (page précédente) soit un automorphisme de groupe.

Exercice 1.1.5.16 Soit $\vec{u} \in \mathbb{R}^3$ fixé et soit $f : \mathbb{R}^3 \longrightarrow \mathbb{R}^3$ définie par :

$$\forall \vec{x} \in \mathbb{R}^3 \ , \ f(\vec{x}) = \vec{u} \wedge \vec{x}$$

1. Montrer que f est un endomorphisme de $(\mathbb{R}^3, +)$.
2. Déterminer le noyau de f.
3. f est-elle un automorphisme de $(\mathbb{R}^3, +)$?

Proposition 1.1.5.17 *Soient G et H deux groupes et soit $f : G \longrightarrow H$. On suppose que f est un isomorphisme de groupes. Alors sa bijection réciproque $f^{-1} : H \longrightarrow G$ est aussi un isomorphisme de groupes.*

Preuve :

On sait déjà que f^{-1} est bijective. Il reste donc à montrer que f^{-1} est un morphisme de groupes.

Soient $h, h' \in H$. Montrons que $f^{-1}(h \diamond h') = f^{-1}(h) \star f^{-1}(h')$. Pour cela, on remarque que, puisque f est un morphisme de groupes,

$$f\left(f^{-1}(h) \star f^{-1}(h')\right) = f(f^{-1}(h)) \diamond f(f^{-1}(h'))$$

d'où

$$f\left(f^{-1}(h) \star f^{-1}(h')\right) = h \diamond h' \quad (\text{puisque } f \circ f^{-1} = \mathrm{Id}_H)$$

Par suite, en prenant les images par f^{-1}, on obtient :

$$f^{-1}(h \diamond h') = f^{-1}(h) \star f^{-1}(h')$$

⊠

Proposition 1.1.5.18 *Soient G, H, K trois groupes et soient $f : G \longrightarrow H$ et $g : H \longrightarrow K$. On suppose que f et g sont deux morphismes de groupes.*
Alors $g \circ f : G \longrightarrow K$ est un morphisme de groupes.

Preuve :

On note $\star$ la loi de G, $\diamond$ la loi de H et $\times$ la loi de K.
L'application $g \circ f$ est bien définie. Soient $x, x' \in G$. On a alors :

$$(g \circ f)(x \star x') = g(f(x) \diamond f(x'))$$

car f est un morphisme de groupes. De plus,

$$g(f(x) \diamond f(x')) = g(f(x)) \times g(f(x'))$$

car g est un morphisme de groupes. Par suite,

$$(g \circ f)(x \star x') = (g \circ f)(x) \times (g \circ f)(x')$$

Ce qui prouve que $g \circ f$ est bien un morphisme de groupes.

⊠

1.2 Anneaux et corps

1.2.1 Définitions

Définition 1.2.1.1 Soit A un ensemble non vide muni de deux lois de composition internes, notées respectivement additivement et multiplicativement. On dit que $(A, +, \times)$ est un anneau si :

(i) $(A, +)$ est un groupe abélien ;

(ii) $\times$ est associative et admet un élément neutre 1_A ;

(iii) $\times$ est distributive (à droite et à gauche) par rapport à $+$, c'est-à-dire :

$$\begin{aligned} \forall (x, y, z) \in A^3 \ , \ x \times (y + z) &= (x \times y) + (x \times z) \\ \forall (x, y, z) \in A^3 \ , \ (x + y) \times z &= (x \times z) + (y \times z) \end{aligned}$$

Lorsque $\times$ est commutative, on dit que A est un anneau commutatif.

Définition 1.2.1.2 On dit qu'un ensemble $\mathbb{K}$ muni de deux lois de composition internes, notées respectivement additivement et multiplicativement est un corps si :

(i) $(\mathbb{K}, +, \times)$ est un anneau non réduit à $\{0_\mathbb{K}\}$ $(\mathbb{K} \neq \{0_\mathbb{K}\})$;

(ii) tout élément non nul est inversible pour la loi $\times$, ou encore $(\mathbb{K}^\star, \times)$ est un groupe, avec $\mathbb{K}^\star = \mathbb{K} \setminus \{0_\mathbb{K}\}$.

⚠ **Attention :** quand on dit que $(A, +, \times)$ est un anneau, l'ordre des lois de composition est important ! $(A, \star, \diamond)$ est un anneau n'est pas du tout équivalent à $(A, \diamond, \star)$ est un anneau !

Exemple 1.2.1.3 Les exemples suivants sont des anneaux ou des corps de référence :

- $(\mathbb{Z}, +, \times)$ est un anneau commutatif mais n'est pas un corps ;
- $(\mathbb{Q}, +, \times)$, $(\mathbb{R}, +, \times)$ et $(\mathbb{C}, +\times)$ sont des corps commutatifs ;
- $(\mathcal{C}^0(\mathbb{R}), +, \times)$ est un anneau commutatif mais n'est pas un corps ;
- l'ensemble des polynômes muni de l'addition et de la multiplication « usuelles » est un anneau commutatif ;
- l'ensemble $\mathcal{F}(\mathbb{R}, \mathbb{R})$ muni de l'addition de fonctions et de la multiplication usuelle entre fonctions est un anneau commutatif mais n'est pas un corps.

Exemple 1.2.1.4 Par contre, $(\mathcal{F}(\mathbb{R},\mathbb{R}),+,\circ)$ n'est pas un anneau puisque la loi $\circ$ (la composition) n'est pas distributive à droite par rapport à l'addition $+$.

Remarque : *il existe bien des anneaux non commutatifs et des corps non commutatifs mais les exemples « simples » sont plus faciles à construire lorsque les matrices ont déjà été définies (voir cours de mathématiques supérieures 2). On peut cependant construire un exemple simple lié aux matrices : c'est l'objet de l'exercice suivant.*

Exercice 1.2.1.5 Soit $G = \{0_G, 1_G\}$ muni de la loi $+$ définie par :

$$0_G + 0_G = 0_G \ ; \ 0_G + 1_G = 1_G + 0_G = 1_G \text{ et } 1_G + 1_G = 0_G$$

1. Vérifier que $(G,+)$ est un groupe commutatif.
2. Montrer que $V = G \times G$ muni de la loi $+_V$ définie par :

$$\forall (x,y) \in V \ , \ \forall (x',y') \in V \ , \ (x,y) +_V (x',y') = (x+x', y+y')$$

   est un groupe commutatif.
3. Pour $f, g \in \mathrm{End}(V)$, on définit $f \oplus g$ par la relation :

$$\forall (x,y) \in V \ , \ (f \oplus g)((x,y)) = f((x,y)) + g((x,y))$$

   Démontrer que $(\mathrm{End}(V), \oplus, \circ)$ est un anneau et qu'il est non commutatif.

Cet exemple correspond à l'ensemble $\mathcal{M}_2(\mathbb{F}_2)$ (matrices carrées de taille 2 à coefficients dans $\mathbb{F}_2$ (le corps commutatif à deux éléments)) dont on sait qu'il s'agit d'un anneau non commutatif.

1.2.2 Sous-anneaux et sous-corps

Définition 1.2.2.1 Soit A un anneau. On dit qu'une partie $B \subset A$ est un sous-anneau de A si :

(i) $(B,+)$ est un sous-groupe de $(A,+)$;

(ii) $1_A \in B$;

(iii) B est stable par $\times$: $\forall (x,y) \in B^2$, $x \times y \in B$.

Exemple 1.2.2.2 Il est clair que $(\mathbb{Z},+,\times)$ est un sous-anneau de $(\mathbb{Q},+,\times)$.

Exercice 1.2.2.3 L'ensemble $(2\mathbb{Z},+,\times)$ est-il un sous-anneau de $(\mathbb{Z},+,\times)$?

Exemple 1.2.2.4 L'ensemble $\mathcal{C}^0(\mathbb{R})$ des fonctions continues sur $\mathbb{R}$ à valeurs réelles est un sous-anneau de l'ensemble des applications de $\mathbb{R}$ dans $\mathbb{R}$. En effet,

- $\mathcal{C}^0(\mathbb{R}) \subset \mathcal{F}(\mathbb{R},\mathbb{R})$;
- $(\mathcal{C}^0(\mathbb{R}),+)$ est un sous-groupe de $(\mathcal{F}(\mathbb{R},\mathbb{R}),+)$ car :
  - $0_{\mathcal{F}(\mathbb{R},\mathbb{R})}$ (la fonction constante sur $\mathbb{R}$ égale à $0_{\mathbb{R}}$) est continue sur $\mathbb{R}$ donc $0_{\mathcal{F}(\mathbb{R},\mathbb{R})} \in \mathcal{C}^0(\mathbb{R})$;
  - si f et g sont continues sur $\mathbb{R}$, alors $f-g$ est aussi continue sur $\mathbb{R}$, c'est-à-dire :

$$\forall (f,g) \in \mathcal{C}^0(\mathbb{R})^2 \ , \ f-g \in \mathcal{C}^0(\mathbb{R})$$

- $1_{\mathcal{F}(\mathbb{R},\mathbb{R})}$ (fonction constante égale à $1_{\mathbb{R}}$) est continue donc $1_{\mathcal{F}(\mathbb{R},\mathbb{R})} \in \mathcal{C}^0(\mathbb{R})$;
- et enfin, si $f,g \in \mathcal{C}^0(\mathbb{R})$, alors $f \times g \in \mathcal{C}^0(\mathbb{R})$ (un produit de fonctions continues est continu).

Exercice 1.2.2.5 L'ensemble des fonctions paires (définies sur $\mathbb{R}$) est-il un sous-anneau de l'ensemble $\mathcal{F}(\mathbb{R},\mathbb{R})$? Même question pour l'ensemble des fonctions impaires.

Proposition 1.2.2.6 *Soient A un anneau et B un sous-anneau de A. Alors $(B,+,\times)$ est un anneau.*

Preuve :

C'est évident mais on va néanmoins le justifier.

• $(B,+)$ est un sous-groupe de $(A,+)$ donc $(B,+)$ est un groupe abélien.

• L'application $\times : B \times B \longrightarrow B$ est une application bien définie (propriété (iii) de la définition) : c'est donc une loi de composition interne sur B.

• $1_A \in B$ et 1_A est neutre pour $\times$ dans A : $\forall x \in A$, $1_A \times x = x \times 1_A = x$.
Or, $B \subset A$ donc nécessairement : $\forall x \in B$, $1_A \times x = x \times 1_A = x$.
Autrement dit, 1_A est l'élément neutre dans B pour $\times$.

• Puisque $\times$ est associative sur A, sa restriction à B l'est aussi. En clair :

$$\forall (x,y,z) \in A^3 \ , \ (x \times y) \times z = x \times (y \times z)$$

a fortiori : $\forall (x,y,z) \in B^3$, $(x \times y) \times z = x \times (y \times z)$

• De même, puisque $\times$ est distributive par rapport à $+$ sur A, elle l'est sur B.

$\boxtimes$

Proposition 1.2.2.7 (Caractérisation des sous-anneaux) *Soient A un anneau et $B \subset A$. Alors B est un sous-anneau de A si et seulement si il vérifie les propriétés suivantes :*

(i) $1_A \in B$;

(ii) $\forall (x,y) \in B^2$, $x - y \in B$;

(iii) $\forall (x,y) \in B^2$, $x \times y \in B$.

Preuve :

• Montrons $\Longrightarrow$

On suppose que B est un sous-anneau de A.
Alors, par définition, les propriétés (i) et (iii) sont vérifiées.
Par ailleurs, soient $x, y \in B$. Par hypothèse, $(B,+)$ est un sous-groupe de $(A,+)$. Par suite, $x - y \in B$ et donc (ii) est également vérifiée.

• Montrons $\Longleftarrow$

On suppose que B vérifie les propriétés (i), (ii) et (iii). Montrons que B est un sous-anneau de A. En fait, il reste seulement à montrer que $(B,+)$ est un sous-groupe de $(A,+)$. Or, par hypothèse :

- $B \neq \emptyset$ (puisque $1_A \in B$) ;
- et $\forall (x,y) \in B^2$, $x - y \in B$.

Par conséquent, $(B,+)$ est un sous-groupe de $(A,+)$.

$\boxtimes$

Remarque : *dans la pratique, on ne montre presque jamais qu'un ensemble B est un anneau. Comme pour les groupes, on montre que c'est un sous-anneau d'un anneau de référence. Ceci permet d'éviter les vérifications fastidieuses pour l'associativité et la distributivité. On fera le point sur les méthodes pour prouver qu'un ensemble est un anneau à la fin de ce chapitre.*

Définition 1.2.2.8 Soit $(\mathbb{L}, +, \times)$ un corps. On dit qu'une partie $\mathbb{K} \subset \mathbb{L}$ est un sous-corps de $\mathbb{L}$ si :

(i) $\mathbb{K}$ est un sous-anneau de $\mathbb{L}$;

(ii) $\forall x \in \mathbb{K}^\star$, $x^{-1} \in \mathbb{K}$.

Proposition 1.2.2.9 (Caractérisation des sous-corps) *Soient $(\mathbb{L}, +, \times)$ un corps et $\mathbb{K} \subset \mathbb{L}$. Alors $\mathbb{K}$ est un sous-corps de $\mathbb{L}$ si et seulement si il vérifie les propriétés suivantes :*

(i) $1_{\mathbb{L}} \in \mathbb{K}$;

(ii) $\forall (x, y) \in \mathbb{K}^2$, $x - y \in \mathbb{K}$;

(iii) $\forall (x, y) \in \mathbb{K}^2$, $x \times y \in \mathbb{K}$;

(iv) $\forall x \in \mathbb{K}^\star$, $x^{-1} \in \mathbb{K}$.

Preuve :

C'est évident car les conditions (i), (ii) et (iii) sont équivalentes à $\mathbb{K}$ est un sous-anneau de $\mathbb{L}$ (d'après la caractérisation des sous-anneaux). ⊠

Remarque : *dans la proposition précédente, on peut remplacer les propriétés (iii) et (iv) par la condition :*

$$\forall (x, y) \in \mathbb{K}^\star \times \mathbb{K}^\star \ , \ x \times y^{-1} \in \mathbb{K}$$

Mais cela nécessite les règles de calcul dans un anneau qu'on étudiera dans le paragraphe suivant.

1.2.3 Règles de calcul dans un anneau

Remarque sur les notations : *si $(A, +, \times)$ est un anneau et si $(x, y) \in A^2$, on note abusivement :*

$$x \times y = xy$$

c'est-à-dire qu'on omet l'opération $\times$. En fait, c'est comme pour les réels où l'absence de symbole entre deux éléments x et y sous-entend que c'est le produit.

De même, si $(G, \cdot)$ est un groupe, la notation xy est utilisée pour désigner $x \cdot y$.

Proposition 1.2.3.1 *Soit $(A, +, \times)$ un anneau. Alors :*

(i) $\forall x \in A$, $0_A \times x = x \times 0_A = 0_A$;

(ii) on a la "règle des signes" :

$$\forall (x, y) \in A^2 \ , \ (-x) \times y = x \times (-y) = -(x \times y)$$

$$\forall (x, y) \in A^2 \ , \ (-x) \times (-y) = x \times y$$

Preuve :

• Montrons (i). Soit $x \in A$. Alors :

$$x \times 0_A = x \times (0_A + 0_A) = x \times 0_A + x \times 0_A$$

Or, $(A, +)$ est un groupe, on peut ajouter l'opposé de $x \times 0_A$ à chaque terme, ce qui donne :

$$0_A = x \times 0_A$$

On démontre la seconde égalité de la même façon.

• Montrons (ii). Soit $(x, y) \in A^2$. Alors :

$$0_A = x \times 0_A = x \times (y - y) = x \times y + x \times (-y)$$

Par suite, en ajoutant l'opposé de $x \times y$, on obtient :

$$x \times (-y) = -(x \times y)$$

On prouve les autres égalités de la même façon. ⊠

Définition 1.2.3.2 Soit A un anneau non trivial (c'est-à-dire tel que $0_A \neq 1_A$). On dit que A est un anneau intègre si :

$$\forall (x, y) \in A^2 \ , \ (x \times y = 0_A \Longrightarrow x = 0_A \quad \text{ou} \quad y = 0_A)$$

Si a et b sont des éléments non nuls de A tels que $a \times b = 0$, on dit que a et b sont des diviseurs de zéro.

Exemple 1.2.3.3 $\mathbb{Z}$ est un anneau intègre. De même, $\mathbb{Q}$, $\mathbb{R}$ et $\mathbb{C}$ sont des anneaux intègres.

Exemple 1.2.3.4 En revanche, il existe des anneaux qui ne sont pas intègres. Par exemple, si on considère l'anneau A des fonctions continues sur $\mathbb{R}$ (muni de l'addition $+$ et de la multiplication $\times$ des fonctions) et on définit :

$$\forall x \in \mathbb{R} \ , \ f(x) = \begin{cases} x & \text{si } x \geqslant 0 \\ 0 & \text{sinon} \end{cases} \quad \text{et} \quad \forall x \in \mathbb{R} \ , \ g(x) = \begin{cases} x & \text{si } x \leqslant 0 \\ 0 & \text{sinon} \end{cases}$$

Alors, on vérifie sans peine que f et g sont bien continues sur $\mathbb{R}$ (et donc $(f, g) \in A^2$) et pour tout réel x, $f(x) \times g(x) = 0$, c'est-à-dire $f \times g = 0_A$. Pourtant, ni f, ni g ne sont identiquement nulles, c'est-à-dire $f \neq 0_A$ et $g \neq 0_A$.

⚠ **Attention :** on retient donc que dans un anneau quelconque, la « règle habituelle » qui dit « qu'un produit est nul si et seulement si l'un au moins des facteurs est nul » est fausse ! Autrement dit,

$$\begin{array}{rcll} (x = 0_A \text{ ou } y = 0_A) & \Longrightarrow & x \times y = 0_A & \text{est vraie} \\ x \times y = 0_A & \Longrightarrow & (x = 0_A \text{ ou } y = 0_A) & \underline{\textbf{est fausse en général}} \end{array}$$

Les anneaux pour lesquels cette propriété est vraie sont des anneaux particuliers qu'on vient de définir, à savoir les anneaux intègres.

En revanche, il y a un cas particulier important, c'est l'objet de la proposition suivante.

Proposition 1.2.3.5 *Si $\mathbb{K}$ est un corps, alors $\mathbb{K}$ est un anneau intègre.*

Preuve :

On commence par un petit rappel de logique qui est très important :

$$A \Longrightarrow (B \vee C) \quad \equiv \quad (A \wedge \rceil B) \Longrightarrow C$$

Ainsi, ici, il s'agit de prouver la propriété suivante :

$$\forall (x, y) \in \mathbb{K}^2 \ , \ ((x \times y = 0_{\mathbb{K}} \ \wedge \ x \neq 0_{\mathbb{K}}) \Longrightarrow y = 0_{\mathbb{K}})$$

Soient $x \in \mathbb{K}$ et $y \in \mathbb{K}$ tels que $x \times y = 0_{\mathbb{K}}$ et $x \neq 0_{\mathbb{K}}$. Alors, comme $x \neq 0_{\mathbb{K}}$, x admet un inverse pour la loi $\times$ (par définition d'un corps). On a alors en multipliant l'égalité $x \times y = 0_{\mathbb{K}}$ à gauche par x^{-1} :

$$x^{-1} \times (x \times y) = x^{-1} \times 0$$

c'est-à-dire $y = 0_{\mathbb{K}}$.

⊠

Définition 1.2.3.6 Soit $(A, +, \times)$ un anneau. On dit qu'un élément $x \in A$ est inversible si x admet un inverse pour $\times$ dans A, c'est-à-dire s'il existe $y \in A$ tel que $x \times y = y \times x = 1_A$. L'ensemble des éléments inversibles de A est noté $A^\star$.

Exercice 1.2.3.7 Soit $(A, +, \times)$ un anneau.

1. Montrer que $(A^\star, \times)$ est un groupe. $(A^\star, \times)$ est-il un sous-groupe de $(A, \times)$?
2. $(A^\star, +, \times)$ est-il un corps ?

Théorème 1.2.3.8 (Binôme de Newton) *Soit $(A, +\times)$ un anneau (pas forcément commutatif) et soient x, y deux éléments de A. On suppose que $x \times y = y \times x$ (c'est-à-dire x et y commutent). Alors pour tout entier $n \in \mathbb{N}$:*

$$(x+y)^n = \sum_{k=0}^{n} \binom{n}{k} x^k y^{n-k}$$

avec la convention que $a^0 = 1_A$ pour tout élément $a \in A$.

Preuve :

On démontre la propriété par récurrence sur $n \in \mathbb{N}$.

Initialisation :

Pour $n = 0$, $(x+y)^0 = 1_A = \binom{0}{0} x^0 y^0 = \sum_{k=0}^{0} \binom{0}{k} x^k y^{0-k}$.

Ce qui prouve que la propriété est vraie au rang 0.

Hérédité :

On suppose la propriété vraie au rang $n \in \mathbb{N}$; montrons qu'elle est encore vraie au rang $n+1$. On a successivement :

$$\begin{aligned}
(x+y)^{n+1} &= (x+y) \times (x+y)^n \\
&= (x+y) \times \sum_{p=0}^{n} \binom{n}{p} x^p y^{n-p} \quad \text{(hypothèse de récurrence)} \\
&= \sum_{p=0}^{n} \binom{n}{p} x^{p+1} y^{n-p} \; + \; \sum_{p=0}^{n} \binom{n}{p} x^p y^{n+1-p} \\
&= \sum_{k=1}^{n+1} \binom{n}{k-1} x^k y^{n+1-k} \; + \; \sum_{p=0}^{n} \binom{n}{p} x^p y^{n+1-p}
\end{aligned}$$

(on a fait le changement d'indice $k = p+1$ dans la première somme).

Or, d'une part :

$$\sum_{k=1}^{n+1} \binom{n}{k-1} x^k y^{n+1-k} = \binom{n}{n} x^{n+1} + \sum_{k=1}^{n} \binom{n}{k-1} x^k y^{n+1-k}$$

et d'autre part :

$$\sum_{p=0}^{n} \binom{n}{p} x^p y^{n+1-p} = \sum_{k=1}^{n} \binom{n}{k} x^k y^{n+1-k} + \binom{n}{0} y^{n+1}$$

Par suite,

$$\begin{aligned}(x+y)^{n+1} &= y^{n+1} + \sum_{k=1}^{n} \left(\binom{n}{k-1} + \binom{n}{k} \right) x^k y^{n+1-k} + x^{n+1} \\ &= \binom{n+1}{0} x^0 y^{n+1} + \sum_{k=1}^{n} \binom{n+1}{k} x^k y^{n+1-k} + \binom{n+1}{n+1} x^{n+1} y^0 \\ &= \sum_{k=0}^{n+1} \binom{n+1}{k} x^k y^{n+1-k}\end{aligned}$$

Ce qui montre que la propriété est vraie au rang $n+1$ et achève la récurrence.

⊠

⚠ **Attention :** la formule du binôme ne s'applique pas lorsque $a \times b \neq b \times a$. On reverra des exemples plus tard, dans le chapitre sur les endomorphismes d'un espace vectoriel (ou dans l'anneau des matrices carrées).

Proposition 1.2.3.9 *Soit $(A, +, \times)$ un anneau et soit $(x, y) \in A^2$. On suppose que x et y commutent (c'est-à-dire $x \times y = y \times x$), alors pour tout entier $n \in \mathbb{N}^\star$:*

$$x^n - y^n = (x - y) \times \left(\sum_{k=0}^{n-1} x^k \times y^{n-1-k} \right)$$

Exercice 1.2.3.10 Démontrer cette proposition.

Exercice 1.2.3.11 Soit $(A, +, \times)$ un anneau et soit $y \in A$. On suppose que y est nilpotent, c'est-à-dire qu'il existe un entier $n \in \mathbb{N}^\star$ tel que $y^n = 0_A$. En utilisant la proposition précédente, montrer que $1 - y$ est inversible et déterminer son inverse.

1.2.4 Opérations sur les sous-anneaux et sous-corps

Proposition 1.2.4.1 *Soient A un anneau (respectivement un corps), B et C deux sous-anneaux (respectivement sous-corps) de A. Alors $B \cap C$ est un sous-anneau (respectivement sous-corps) de A.*

Preuve :

Il suffit d'appliquer la proposition de caractérisation des sous-anneaux (respectivement sous-corps) et c'est immédiat.

⊠

De même que pour les groupes, on peut généraliser cette propriété à une intersection quelconque (exercice : faire la preuve).

Proposition 1.2.4.2 *Soit A un anneau (respectivement un corps) et soit $(B_i)_{i\in I}$ une famille quelconque (finie ou infinie) de sous-anneaux (respectivement sous-corps) de A. Alors, $\bigcap_{i\in I} B_i$ est un sous-anneau (respectivement sous-corps) de A.*

1.2.5 Morphismes d'anneaux (ou de corps)

Définition 1.2.5.1 Soient $(A, +, \times)$ et $(B, \oplus, \otimes)$ deux anneaux.
On dit qu'une application $f : A \longrightarrow B$ est un morphisme d'anneaux si :

(i) $\forall (x, y) \in A^2$, $f(x + y) = f(x) \oplus f(y)$;

(ii) $f(1_A) = 1_B$;

(iii) $\forall (x, y) \in A^2$, $f(x \times y) = f(x) \otimes f(y)$.

Remarque : *lorsque A et B sont des corps, un morphisme de corps est une application de A dans B qui est un morphisme de l'anneau A dans l'anneau B.*

Définition 1.2.5.2 Soient $(A, +, \times)$ et $(B, \oplus, \otimes)$ deux anneaux (respectivement corps).

- On dit qu'une application $f : A \longrightarrow B$ est un isomorphisme d'anneaux (respectivement de corps) si f est un morphisme d'anneaux et f est bijective.
- On dit qu'une application $f : A \longrightarrow A$ est un endomorphisme d'anneau (respectivement de corps) si f est un morphisme d'anneaux.
- On dit qu'une application $f : A \longrightarrow A$ est un automorphisme de l'anneau A (respectivement du corps A) si f est un endomorphisme de l'anneau A (respectivement du corps A) et si f est bijective.

Remarques :

- *ainsi, un automorphisme de l'anneau A est un endomorphisme d'anneau et un isomorphisme de A dans lui-même ;*
- *si $f : A \longrightarrow B$ est un morphisme d'anneaux, alors f est aussi un morphisme de groupes de $(A, +)$ dans $(B, +)$. En particulier, le noyau et l'image de f sont encore définis par :*

$$\ker(f) = f_r^{-1}(\{0_B\}) \quad et \quad \mathrm{Im} f = f_d(A)$$

Exemple 1.2.5.3 La conjugaison complexe est un automorphisme du corps $\mathbb{C}$. En effet,

- $\forall (z, z') \in \mathbb{C}^2$, $\overline{z + z'} = \overline{z} + \overline{z'}$;
- $\overline{1_{\mathbb{C}}} = 1_{\mathbb{C}}$;
- $\forall (z, z') \in \mathbb{C}^2$, $\overline{z \times z'} = \overline{z} \times \overline{z'}$;
- et enfin, la conjugaison est bien une application bijective de $\mathbb{C}$ dans lui-même.

Exemple 1.2.5.4 L'application $\varphi : \begin{array}{ccc} \mathcal{F}(\mathbb{R}, \mathbb{R}) & \longrightarrow & \mathbb{R} \\ f & \longmapsto & f(0) \end{array}$ est un morphisme d'anneaux, mais n'est pas un isomorphisme d'anneaux. En effet,

- $\forall (f, g) \in \mathcal{F}(\mathbb{R}, \mathbb{R})^2$, $\varphi(f + g) = (f + g)(0) = f(0) + g(0) = \varphi(f) + \varphi(g)$;
- $\varphi(1_{\mathcal{F}(\mathbb{R},\mathbb{R})}) = 1_{\mathcal{F}(\mathbb{R},\mathbb{R})}(0) = 1_{\mathbb{R}}$;
- $\forall (f, g) \in \mathcal{F}(\mathbb{R}, \mathbb{R})^2$, $\varphi(f \times g) = (f \times g)(0) = f(0) \times g(0) = \varphi(f) \times \varphi(g)$.

Ce qui prouve que φ est bien un morphisme d'anneaux. En revanche, il est clair que φ n'est pas bijective car par exemple, $\varphi(x \longmapsto x) = 0$ donc $\ker \varphi \neq \{0_{\mathcal{F}(\mathbb{R},\mathbb{R})}\}$.

Exercice 1.2.5.5 Soit f un endomorphisme du corps $\mathbb{Q}$.

1. Montrer que : $\forall n \in \mathbb{N}$, $f(n) = n$.
2. Montrer que f est impaire et en déduire que : $\forall n \in \mathbb{Z}$, $f(n) = n$.
3. Pour $p \in \mathbb{N}^\star$, calculer $f(p^{-1})$ en fonction de p.
4. En déduire que $f = \mathrm{Id}_{\mathbb{Q}}$.
5. Que vient-on de prouver ?

Exercice 1.2.5.6 En vous inspirant de l'exercice précédent, déterminer :

1. tous les endomorphismes du groupe $(\mathbb{Z}, +)$;
2. tous les endomorphismes de l'anneau $(\mathbb{Z}, +, \times)$.

De la même façon que pour les morphismes de groupes, on a les propriétés élémentaires suivantes pour les morphismes d'anneaux.

Proposition 1.2.5.7 *Soient A, B et C trois anneaux et soient $f : A \longrightarrow B$ et $g : B \longrightarrow C$ deux morphismes d'anneaux. Alors $g \circ f$ est un morphisme d'anneaux de A dans C.*
Autrement dit, la composée de deux morphismes d'anneaux est encore un morphisme d'anneaux.

Preuve :

On note abusivement $+$ et $\times$ les opérations dans A, B et C.

• Puisque f et g sont des morphismes d'anneaux, f est aussi un morphisme de groupes de $(A, +)$ dans $(B, +)$ et de même g est un morphisme de groupes de $(B, +)$ dans $(C, +)$. D'après les propriétés des morphismes de groupes, $g \circ f$ est un morphisme de groupes de $(A, +)$ dans $(C, +)$.

• Par ailleurs, puisque f et g sont des morphismes d'anneaux, $f(1_A) = 1_B$ et $g(1_B) = 1_C$. Par suite :

$$(g \circ f)(1_A) = g(f(1_A)) = g(1_B) = 1_C$$

• Enfin, soit $(x, y) \in A^2$.

$$\begin{aligned}(g \circ f)(x \times y) &= g(f(x \times y)) \\ &= g(f(x) \times f(y)) \\ &= g(f(x)) \times g(f(y)) \\ &= (g \circ f)(x) \times (g \circ f)(y)\end{aligned}$$

Ce qui prouve que $g \circ f$ est bien un morphisme d'anneaux.

⊠

Remarque : *dans la proposition précédente, si on suppose que A, B et C sont des corps, alors par définition $g \circ f$ est un morphisme de corps.*

Proposition 1.2.5.8 *Soit $f : A \longrightarrow B$ un isomorphisme d'anneaux. Alors f^{-1} est un isomorphisme d'anneaux.*

Preuve :

• Puisque f est bijective et $f(1_A) = 1_B$, $f^{-1}(1_B) = 1_A$.

• D'après les propriétés des morphismes de groupes, on sait déjà que f^{-1} est un morphisme de groupes de $(B, +)$ dans $(A, +)$.

• De plus, pour $(x, y) \in B^2$,

$$\begin{aligned} f^{-1}(x \times y) &= f^{-1}\left(f(f^{-1}(x)) \times f(f^{-1}(y))\right) \\ &= f^{-1}\left(f\left(f^{-1}(x) \times f^{-1}(y)\right)\right) \\ &= \left(f^{-1} \circ f\right)\left(f^{-1}(x) \times f^{-1}(y)\right) \\ &= f^{-1}(x) \times f^{-1}(y) \end{aligned}$$

• Enfin, f^{-1} est également bijective.

Ce qui prouve que f^{-1} est un isomorphisme d'anneaux.

⊠

Proposition 1.2.5.9 *Soit $A \xrightarrow{f} B$ un morphisme d'anneaux. Alors :*

(i) $\ker(f)$ *est un sous-groupe de $(A, +)$ mais n'est pas un sous-anneau de A (sauf si $0_B = 1_B$) ;*

(ii) $\mathrm{Im}(f)$ *est un sous-anneau de B.*

Preuve :

La démonstration est laissée en exercice.

⊠

▶ Méthode :

Pour démontrer qu'un ensemble A est un anneau, on peut :

1. montrer que c'est l'image d'un morphisme d'anneaux ;
2. montrer que c'est un sous-anneau d'un anneau connu (pour cela, on utilise la caractérisation des sous-anneaux) ;
3. montrer que c'est une intersection de sous-anneaux ;
4. revenir à la définition formelle d'un anneau.

1.3 Exercices

Exercice 1.3.1 Soit $*$ la loi de composition interne définie sur $\mathbb{R}$ par :

$$\forall (x,y) \in \mathbb{R}^2 \ , \ x * y = x + y + x^2 y$$

1. Vérifier que $*$ n'est pas commutative, n'est pas associative, que $*$ admet un élément neutre et qu'aucun élément de $\mathbb{R} \setminus \{0\}$ n'admet d'inverse pour $*$.
2. Résoudre les équations suivantes d'inconnue $x \in \mathbb{R}$: $2 * x = -3$ puis $x * x = 3$.

Exercice 1.3.2 Montrer que $\mathbb{R}^2$ muni de la loi $(x,y) * (x',y') = (x + x', ye^{x'} + y'e^{-x})$ est un groupe non-abélien.

Exercice 1.3.3 Soit la loi de composition $\star$ définie sur $\mathbb{R}$ par :

$$\forall (x,y) \in \mathbb{R}^2 \ , \ x \star y = \sqrt[3]{x^3 + y^3}$$

1. Montrer que $(\mathbb{R}, \star)$ est un groupe.
2. L'application $f : (\mathbb{R}, \star) \longrightarrow (\mathbb{R}, +)$ définie par $f(x) = x^3$ est-elle un morphisme de groupes ?

Exercice 1.3.4 Soit E un ensemble non vide. On définit la loi $\bigtriangleup$ sur $\mathcal{P}(E)$ par :

$$\forall (A,B) \in \mathcal{P}(E) \times \mathcal{P}(E) \ , \ A \bigtriangleup B = (A \setminus B) \cup (B \setminus A)$$

Montrer que $(\mathcal{P}(E), \bigtriangleup)$ est un groupe abélien.

Exercice 1.3.5 Montrer que l'ensemble $\{z \in \mathbb{C} \ , \ \exists n \in \mathbb{N}^\star \ , \ z^n = 1\}$ muni de la multiplication est un groupe.

Exercice 1.3.6 Soient G un groupe et H, K deux sous-groupes de G. Montrer que $H \cup K$ est un sous-groupe de G si et seulement si $K \subset H$ ou $H \subset K$.

Exercice 1.3.7 Soit G un ensemble non vide, muni d'une loi de composition interne $\star$ associative. On suppose qu'il existe un élément $e \in G$ tel que :

$$\begin{cases} \forall x \in G \ , \ x \star e = x \\ \forall x \in G \ , \ \exists y \in G \ , \ x \star y = e \end{cases}$$

Montrer que $(G, \star)$ est un groupe.

Exercice 1.3.8 Soit G un groupe tel que : $\forall g \in G$, $g^2 = e$.

1. Montrer que G est abélien.
2. Montrer que si H est un sous-groupe de G et $a \in G \setminus H$, alors $H \cup aH$ est un sous-groupe de G et $H \cap aH = \emptyset$.
3. **(Difficile)** Déduire de la question précédente que si G est fini, alors son cardinal est une puissance de 2.

Exercice 1.3.9 Soit G un groupe fini de cardinal pair dont le neutre est noté 1. On veut montrer qu'il existe un élément x de G distinct de 1 et égal à son propre inverse. Pour cela, on pose :

$$A = \{g \in G \mid g \neq 1 \text{ et } g^{-1} = g\} \quad \text{et} \quad B = \{g \in G \mid g \neq 1 \text{ et } g^{-1} \neq g\}$$

1. A et B sont-ils des sous-groupes de G ?
2. Justifier que A et B sont des ensembles finis puis exprimer $|G|$ en fonction de $|A|$ et de $|B|$.
3. Montrer que $|B|$ est pair et conclure.

Exercice 1.3.10 Soit $(G, *)$ un groupe, on note $Z(G)$ le *centre* de G qui est par définition l'ensemble des éléments de G qui commutent avec tous les éléments de G :

$$Z(G) = \{x \in G \ ; \ \forall g \in G, \ x * g = g * x\}$$

1. Dans le cas où G est commutatif, que dire de $Z(G)$?
2. Montrer que $Z(G)$ est un sous-groupe de G.
3. Soient $(G, *)$ et $(H, \times)$ deux groupes et $f : G \to H$ un morphisme de groupes. Montrer que :
   (a) si f est surjectif, alors $f(Z(G)) \subset Z(H)$;
   (b) si f est injectif, alors $f_r^{-1}(Z(H)) \subset Z(G)$.

Exercice 1.3.11 Soit G un groupe. Pour tout $a \in G$, on définit : $f_a : \begin{array}{ccc} G & \longrightarrow & G \\ g & \longmapsto & aga^{-1} \end{array}$.

1. Démontrer que f_a est un automorphisme de G. On note $\mathrm{Int}(G)$ l'ensemble des applications f_a lorsque a décrit G.
2. Montrer que $\varphi : \begin{array}{ccc} G & \longrightarrow & \mathrm{Aut}(G) \\ a & \longmapsto & f_a \end{array}$ est un morphisme de groupes.
3. Quel est le noyau de φ ? Quelle est son image ?
4. En déduire que $(\mathrm{Int}(G), \circ)$ est un groupe.

Exercice 1.3.12 On considère les applications suivantes de $\mathbb{R} \setminus \{0,1\}$ dans lui-même :

$$f_1 : x \longmapsto x \qquad f_2 : x \longmapsto 1-x \qquad f_3 : x \longmapsto \frac{1}{1-x}$$

$$f_4 : x \longmapsto \frac{1}{x} \qquad f_5 : x \longmapsto \frac{x}{x-1} \qquad f_6 : x \longmapsto \frac{x-1}{x}$$

1. Montrer que $G = \{f_i \ , \ 1 \leqslant i \leqslant 6\}$ muni de la loi $\circ$ est un groupe.
2. Déterminer tous les sous-groupes de G.
3. Quel est le plus petit sous-groupe de G contenant f_2 ? Contenant f_3 ? Contenant f_2 et f_3 ?

Exercice 1.3.13 Soient $\mathbb{U}_{12} = \{z \in \mathbb{C} \ / \ z^{12} = 1\}$ l'ensemble des racines 12^{e} de l'unité et soit

$$\begin{array}{rccc} f & : & \mathbb{C}^\star & \longrightarrow & \mathbb{C}^\star \\ & & z & \longmapsto & z^{12}. \end{array}$$

1. Démontrer que $\mathbb{U}_{12}$ est un sous-groupe de $(\mathbb{C}^\star, \times)$.
2. Justifier que $\mathbb{U}_{12}$ est un groupe *monogène*, c'est-à-dire qu'il existe $w \in \mathbb{U}_{12}$ tel que tout élément z de $\mathbb{U}_{12}$ s'écrit $z = w^n$, avec $n \in \mathbb{N}$.
3. Démontrer que f est un endomorphisme du groupe $(\mathbb{C}^\star, \times)$.
4. Déterminer le noyau de f. f est-elle une injection ?
5. f est-elle une surjection ?
6. Soit $\begin{array}{rccc} g : \mathbb{U}_{12} & \longrightarrow & \mathbb{U}_{12} \\ z & \longmapsto & z^4 \end{array}$.
   (a) Justifier que l'application g est bien définie.
   (b) Démontrer que g est un morphisme de groupes.
   (c) Déterminer le noyau de g.
   (d) Déterminer l'image de g.
   (e) Vérifier l'égalité : $|\ker(g)| \times |\mathrm{Im} g| = |\mathbb{U}_{12}|$.

Exercice 1.3.14 On pose $\mathbb{Z}[i] = \{a + ib \ , \ (a,b) \in \mathbb{Z}^2\}$.

1. Montrer que $\mathbb{Z}[i]$ est un sous-anneau de $\mathbb{C}$. S'agit-il d'un corps ?
2. Montrer que la conjugaison est un automorphisme de l'anneau $\mathbb{Z}[i]$.
3. Quels sont les éléments inversibles de $\mathbb{Z}[i]$?

Exercice 1.3.15 Soit P l'ensemble des fonctions paires définies sur $\mathbb{R}$ à valeurs dans $\mathbb{R}$.

1. $(P, +, \times)$ est-il un anneau ? Est-il commutatif ? Est-il un corps ?
2. $(P, +, \circ)$ est-il un anneau ? Est-il commutatif ?

Exercice 1.3.16 Soit $(A, +, \star)$ un anneau intègre. On suppose également que A est un ensemble fini. On rappelle que si f est une application de A dans A (A est un ensemble fini), alors f est injective si et seulement si f est bijective.

1. Soit $a \in A$. Peut-on conclure directement, d'après la définition d'un anneau, que a est inversible pour $\star$?
2. On fixe $a \in A$ avec $a \neq 0_A$. Montrer que l'application $\begin{array}{rccc} \varphi_a : & A & \longrightarrow & A \\ & x & \longmapsto & a \star x \end{array}$ est injective.
3. En déduire que a est inversible à droite.
4. En vous inspirant des questions précédentes, démontrer de même que a est inversible à gauche.
5. Montrer alors que l'inverse à droite est le même que l'inverse à gauche.
6. Que vient-on de démontrer sur A ?

Exercice 1.3.17 Soit A un anneau. Un élément x de A est dit *nilpotent* s'il existe $n \in \mathbb{N}^\star$ tel que $x^n = 0$.

1. Montrer que, si x et y sont nilpotents et commutent, alors $x + y$ est nilpotent.
2. Montrer que, si x est nilpotent et x et y commutent, alors xy est nilpotent.
3. Soit $x \in A$ nilpotent. Montrer que $1 - x$ est inversible et calculer $(1 - x)^{-1}$.

Exercice 1.3.18 On considère les ensembles :

$$\mathbb{Q}[\sqrt{2}] = \{a + b\sqrt{2} \ , \ (a, b) \in \mathbb{Q}^2\} \text{ et } \mathbb{Z}[\sqrt{2}] = \{a + b\sqrt{2} \ , \ (a, b) \in \mathbb{Z}^2\}$$

On rappelle que $\sqrt{2}$ est un irrationnel, résultat qui pourra être utilisé sans démonstration.

1. Montrer que $\forall a, b, a', b' \in \mathbb{Q} \ , \ a + b\sqrt{2} = a' + b'\sqrt{2} \iff (a, b) = (a', b')$.
2. Montrer que $\mathbb{Q}[\sqrt{2}]$ est un sous-corps de $\mathbb{R}$ et que $\mathbb{Z}[\sqrt{2}]$ est un sous-anneau de $\mathbb{Q}[\sqrt{2}]$.
3. À tout $z = a + b\sqrt{2} \in \mathbb{Q}[\sqrt{2}]$, on associe $\bar{z} = a - b\sqrt{2}$. Montrer que l'application $z \longmapsto \bar{z}$ est un automorphisme de $\mathbb{Q}[\sqrt{2}]$.
4. On pose pour $z \in \mathbb{Q}[\sqrt{2}]$, $N(z) = z\bar{z}$.

(a) Montrer que N est multiplicative : $\forall (z,z') \in \mathbb{Q}[\sqrt{2}]^2$, $N(zz') = N(z)N(z')$.

(b) Montrer que $z \in \mathbb{Z}[\sqrt{2}]$ est inversible si et seulement si $N(z) = \pm 1$.

5. À l'aide de la question précédente, déterminer un élément inversible de $\mathbb{Z}[\sqrt{2}]$ distinct de ± 1.

6. Montrer que l'ensemble U des éléments inversibles de $\mathbb{Z}[\sqrt{2}]$ est un groupe pour la loi $\times$.

7. En déduire que U est infini.

8. On pose $U_+ = \{a + b\sqrt{2} \in U \mid a \geqslant 0 \ , \ b \geqslant 0\}$ et $U_+^\star = \{a + b\sqrt{2} \in U_+ \mid b > 0\}$.

   (a) Montrer que : $\forall (a,b) \in \mathbb{Z}^2$, $a + b\sqrt{2} \in U_+^\star \Longrightarrow b \leqslant a < 2b$.

   (b) Soit $z = a + b\sqrt{2} \in U_+^\star$. On pose $z' = z(1+\sqrt{2})^{-1} = a' + b'\sqrt{2}$. Montrer que :

   $$z' \in U_+ \quad \text{et} \quad (0 < a' < a \text{ ou } z' = 1)$$

   (c) En déduire que $U_+ = \{(1+\sqrt{2})^n \ , \ n \in \mathbb{N}\}$.

   (d) Déterminer alors complètement U.

Exercice 1.3.19 Soit G un groupe fini et H un sous-groupe de G. Pour $x \in G$, on note :

$$xH = \{xh \ , \ h \in H\} = \{y \in G \ / \ \exists h \in H \ , \ y = xh\}$$

1. Montrer qu'il existe un entier $n \geqslant 1$ et des éléments $x_1, \cdots, x_n$ de G tels que :

   $$G = \bigcup_{k=1}^{n} x_k H \quad \text{et} \quad \forall i,j \in [\![1,n]\!] \ , \ (\ i \neq j \Longrightarrow x_i H \cap x_j H = \emptyset \ )$$

   On pourra pour cela raisonner par l'absurde et montrer qu'on peut alors construire une famille $(x_n)_{n \in \mathbb{N}^\star}$ d'éléments de G tels que :

   $$\forall (i,j) \in \mathbb{N}^\star \times \mathbb{N}^\star \ , \ (i \neq j \Longrightarrow x_i H \cap x_j H = \emptyset)$$

   et

   $$\bigcup_{k=1}^{n} x_k H \subsetneq G$$

2. En déduire le théorème de Lagrange : *si G est un groupe fini et H un sous groupe de G, alors $|H|$ divise $|G|$.*

3. Application : existe-t-il un sous-groupe de cardinal 14 dans un groupe de cardinal 72 ?

Les exercices suivants font appels à des notions développées dans les chapitres suivants. Pour chaque exercice, il est précisé quelle(s) notion(s) doivent avoir été vues au préalable.

Exercice 1.3.20 *Cet exercice utilise la densité de $\mathbb{Q}$ dans $\mathbb{R}$ (voir chapitre 2, paragraphe 4.8).* Le but de l'exercice est de déterminer tous les morphismes de corps de $\mathbb{R}$ dans $\mathbb{R}$.

1. Donner un exemple de morphisme du corps $\mathbb{R}$ dans lui-même.
2. Soit f un morphisme de corps de $\mathbb{R}$ dans $\mathbb{R}$.
   (a) Déterminer la seule valeur possible pour $f(0)$.
   (b) Montrer que : $\forall x \in \mathbb{N}$, $f(x) = x$.
   (c) Montrer que f est impaire et en déduire que $\forall x \in \mathbb{Z}$, $f(x) = x$.
   (d) En déduire que cela reste vrai pour les rationnels : $\forall x \in \mathbb{Q}$, $f(x) = x$.
   (e) Montrer que f est strictement croissante sur $\mathbb{R}$.
   (f) En utilisant la densité de $\mathbb{Q}$ dans $\mathbb{R}$ ainsi que les variations de f, conclure que : $\forall x \in \mathbb{R}$, $f(x) = x$.

Exercice 1.3.21 *Cet exercice utilise la division euclidienne (voir chapitre 5) et les propriétés de $\mathbb{N}$ (chapitre 2, paragraphe 2.1).* Soit G un groupe cyclique, c'est-à-dire que G est un groupe fini et il existe un élément $g \in G$ tel que :

$$G = \{g^k \ , \ k \in \mathbb{Z}\}$$

1. Soit $n \in \mathbb{N}^\star$ avec $n \geqslant 2$. Donner un exemple de groupe cyclique cardinal n. *On démontrera que l'ensemble donné est bien un groupe cyclique de cardinal n.*
2. Soit G un groupe cyclique de cardinal $n \geqslant 2$. On fixe un élément $g \in G$ tel que $G = \{g^k \ , \ k \in \mathbb{Z}\}$ et on note e l'élément neutre de G.
   (a) Montrer que pour tout entier p, l'ensemble $H_p = \{g^{pk} \ , \ k \in \mathbb{Z}\}$ est un sous-groupe de G.
   (b) Réciproquement, soit H un sous-groupe de G, non réduit à $\{e\}$.
      (i) Montrer que $\{p \in \mathbb{N}^\star \ / \ g^p \in H\}$ admet un plus petit élément, que l'on notera p_0.
      (ii) Montrer que $H_{p_0} \subset H$.
      (iii) Établir que $H \subset H_{p_0}$.

Chapitre 2

Relations, ensembles $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$ et $\mathbb{R}$

Prérequis : dans tout ce chapitre, les notions suivantes sont supposées connues :

- le cours de logique (implications, équivalences, prédicat, récurrence) ;
- notion d'ensemble ;
- applications monotones ; injections, surjections et bijections ;
- structures usuelles : groupes, anneaux et corps ; morphismes de groupes ou d'anneaux.

2.1 Relations

2.1.1 Généralités sur les relations

Définition 2.1.1.1 Soit E un ensemble. Une relation (binaire) sur E, est une forme propositionnelle $P(x, y)$ en deux variables appartenant à E. En appelant $\mathcal{R}$ la relation, on écrit $x\mathcal{R}y$ pour dire que $P(x, y)$ est vraie.

Remarque : *de façon plus formelle, une relation binaire $\mathcal{R}$ sur E est un sous-ensemble de $E \times E$. Pour $(x, y) \in E^2$, on écrit alors $x\mathcal{R}y$ lorsque $(x, y) \in \mathcal{R}$. En notant $P(x, y)$ la propriété $(x, y) \in \mathcal{R}$ et en remarquant qu'un ensemble est caractérisé par la donnée de ses éléments, on a alors :*

$$x\mathcal{R}y \iff P(x, y) \text{ est vraie}$$

Réciproquement, si P est un prédicat sur $E \times E$, en posant

$$\mathcal{R} = \{(x, y) \in E^2 \mid P(x, y) \text{ est vraie}\}$$

on a : $x\mathcal{R}y \iff P(x, y)$ est vraie.

Il y a donc une correspondance (bijective) entre les deux définitions. Seule différence, la première est plus simple à comprendre.

Définition 2.1.1.2 Soit $\mathcal{R}$ une relation (binaire) définie sur E. On dit que $\mathcal{R}$ est :

- réflexive si : $\forall x \in E$, $x\mathcal{R}x$;
- symétrique si : $\forall (x, y) \in E^2$, $(x\mathcal{R}y \Longrightarrow y\mathcal{R}x)$;
- antisymétrique si : $\forall (x, y) \in E^2$, $\Big(\big(x\mathcal{R}y \text{ et } y\mathcal{R}x\big) \Longrightarrow x = y\Big)$;
- transitive si : $\forall (x, y, z) \in E^3$, $\Big(\big(x\mathcal{R}y \text{ et } y\mathcal{R}z\big) \Longrightarrow x\mathcal{R}z\Big)$.

Exemple 2.1.1.3 Soit E l'ensemble des droites du plan. Considérons la relation $\mathcal{R} = \perp$. C'est bien une relation binaire sur E et :

- $\mathcal{R}$ n'est pas réflexive puisque si $\mathcal{D}$ est une droite, $\mathcal{D} \not\perp \mathcal{D}$;
- $\mathcal{R}$ est symétrique puisque si $\mathcal{D}$ et $\mathcal{D}'$ sont deux droites du plan telles que $\mathcal{D} \perp \mathcal{D}'$, alors $\mathcal{D}' \perp \mathcal{D}$;
- $\mathcal{R}$ n'est pas transitive puisque $(\mathcal{D} \perp \mathcal{D}' \text{ et } \mathcal{D}' \perp \mathcal{D}'') \Longrightarrow \mathcal{D} \parallel \mathcal{D}''$ (on est dans le plan).

Exemple 2.1.1.4 Toujours sur l'ensemble E des droites du plan, on considère la relation $\parallel$. Alors, $\parallel$ est une relation :

- clairement réflexive puisque pour toute droite $\mathcal{D}$, $\mathcal{D} \parallel \mathcal{D}$;
- symétrique puisque pour toutes droites $\mathcal{D}$ et $\mathcal{D}'$, $\mathcal{D} \parallel \mathcal{D}' \Longrightarrow \mathcal{D}' \parallel \mathcal{D}$;
- transitive puisque si $\mathcal{D}, \mathcal{D}'$ et $\mathcal{D}''$ sont trois droites telles que $\mathcal{D} \parallel \mathcal{D}'$ et $\mathcal{D}' \parallel \mathcal{D}''$, alors $\mathcal{D} \parallel \mathcal{D}''$.

On reverra un peu plus loin que c'est ce qu'on appelle une relation d'équivalence.

Exemple 2.1.1.5 On considère la relation de divisibilité dans $\mathbb{N}$, c'est-à-dire la relation $\mathcal{R} = |$ définie sur $\mathbb{N}^2$ par :

$$\forall (a,b) \in \mathbb{N}^2 \ , \ a|b \iff \exists n \in \mathbb{N} \ , \ b = na$$

Alors $|$ est une relation réflexive, antisymétrique et transitive sur $\mathbb{N}$. En effet,

- pour tout $a \in \mathbb{N}$, $a = 1_{\mathbb{N}} \times a$ donc $a|a$;
- pour tout $(a,b) \in \mathbb{N}^2$, si $a|b$ et $b|a$, alors il existe $n \in \mathbb{N}$ et $p \in \mathbb{N}$ tels que $b = na$ et $a = pb$. Alors, $b = na = npb$, c'est-à-dire $b(1 - np) = 0$. Par suite,
  - soit $b = 0$ et donc $a = pb = 0$, et *a fortiori* $a = b$;
  - ou bien $np = 1$ et puisque $(n,p) \in \mathbb{N}^2$, $n = p = 1$. Par conséquent, $b = na = a$.
- enfin, si $(a,b,c) \in \mathbb{N}^3$ et $a|b$ et $b|c$. Alors, par définition, il existe deux entiers naturels n et p tels que $b = na$ et $c = pb$. Alors :

  $$c = pb = pna = (pn)a \quad \text{avec } pn \in \mathbb{N}$$

  donc $a|c$.

Exercice 2.1.1.6 Montrer que la relation de divisibilité dans $\mathbb{Z}$, définie par :

$$\forall (a,b) \in \mathbb{Z}^2 \ , \ (a|b \iff \exists n \in \mathbb{Z} \ , \ b = na)$$

est réflexive, transitive mais n'est pas antisymétrique.

Exercice 2.1.1.7 Montrer que si $\mathcal{R}$ est une relation symétrique et antisymétrique, alors :

$$\forall (x,y) \in E^2 \ , \ (x\mathcal{R}y \Longrightarrow x = y)$$

En particulier, si $\mathcal{R}$ est aussi réflexive, alors $x\mathcal{R}y \iff x = y$, c'est-à-dire que $\mathcal{R}$ est la relation d'égalité.

2.1.2 Relation d'ordre

Définition 2.1.2.1 Soit E un ensemble. On dit que $\mathcal{R}$ est une relation d'ordre sur E si $\mathcal{R}$ est réflexive, antisymétrique et transitive. Dans ce cas, on dit que $(E, \mathcal{R})$ est un ensemble ordonné.

Remarques :

- *l'exemple le « plus simple » d'ensemble ordonné est :* $(\mathbb{R}, \leqslant)$ *;*
- *en fait dans cette définition, on veut introduire un « objet » qui permet de « comparer deux éléments » dans l'ensemble* E *: c'est justement la notion de relation d'ordre. La définition posée reprend les propriétés naturelles de la relation* $\leqslant$ *sur l'ensemble des nombres réels ;*
- *un ensemble ordonné est donc un couple* $(E, \mathcal{R})$ *où* E *est un ensemble et* $\mathcal{R}$ *une relation d'ordre sur* E*. Par abus, on dira souvent « soit* E *un ensemble ordonné » au lieu de « soit* $(E, \mathcal{R})$ *un ensemble ordonné » ;*
- *enfin, lorsque* $\mathcal{R}$ *est une relation d'ordre, on la note souvent* $\leqslant$ *au lieu de* $\mathcal{R}$*. Mais il faudra bien faire attention à ne pas confondre ce symbole avec la relation* $\leqslant$ *habituelle dans* $\mathbb{R}$*.*

Exemple 2.1.2.2 $(\mathbb{N}, |)$ (où $|$ est la relation de divisibilité (voir exemple 2.1.1.5)) est un ensemble ordonné. Cette relation correspond bien à « une façon de comparer deux entiers naturels » qui n'est la même que la relation $\leqslant$ usuelle dans $\mathbb{N}$. On peut aussi remarquer que pour la relation d'ordre de divisibilité, on ne peut pas comparer 2 et 3.

Proposition 2.1.2.3 *Soit* X *un ensemble non vide. On définit la relation* $\leqslant$ *sur* $\mathcal{F}(X, \mathbb{R})$ *par :*

$$\forall (f, g) \in \mathcal{F}(X, \mathbb{R})^2 \ , \ f \leqslant g \iff \forall x \in X \ , \ f(x) \leqslant g(x)$$

Alors $(\mathcal{F}(X, \mathbb{R}), \leqslant)$ *est un ensemble ordonné.*

Remarque : *attention, ici il y a bien deux relations* $\leqslant$ *qui sont différentes. La première que l'on vient de définir est une relation d'ordre sur l'ensemble des applications de* X *dans* $\mathbb{R}$ *alors que la deuxième est la relation d'ordre usuelle dans* $\mathbb{R}$*. Si vous pensez confondre ces deux relations distinctes, il est mieux de les noter de façons différentes, comme par exemple* $\leqslant_{\mathbb{R}}$ *pour l'inégalité usuelle dans* $\mathbb{R}$*.*

Preuve :

Pour éviter les confusions (voir remarque précédente), notons $\mathcal{R}$ la relation $\leqslant$ dans l'ensemble des applications de X dans $\mathbb{R}$ et montrons que $(\mathcal{F}(X,\mathbb{R}),\mathcal{R})$ est un ensemble ordonné.

• Montrons que $\mathcal{R}$ est réflexive.

Soit $f \in \mathcal{F}(X,\mathbb{R})$. Alors, pour tout $x \in X$, $f(x) \in \mathbb{R}$. Or, $\leqslant$ est une relation d'ordre sur $\mathbb{R}$: elle est donc réflexive et $f(x) \leqslant f(x)$. Ainsi,

$$\forall x \in X \ , \ f(x) \leqslant f(x)$$

c'est-à-dire $f\mathcal{R}f$. Ce qui prouve que $\mathcal{R}$ est réflexive.

• Montrons que $\mathcal{R}$ est antisymétrique.

Soient f et g deux éléments de $\mathcal{F}(X,\mathbb{R})$ tels que $f\mathcal{R}g$ et $g\mathcal{R}f$. On a alors :

$$\forall x \in X \ , \ f(x) \leqslant g(x) \quad \text{et} \quad \forall x \in X \ , \ g(x) \leqslant f(x)$$

La relation $\leqslant$ étant une relation d'ordre sur $\mathbb{R}$, elle est en particulier antisymétrique. On en déduit que :

$$\forall x \in X \ , \ f(x) = g(x) \quad \text{c'est-à-dire} \quad f = g$$

Ce qui prouve que $\mathcal{R}$ est antisymétrique.

• Montrons que $\mathcal{R}$ est transitive.

Soient f, g et h trois applications de X dans $\mathbb{R}$ vérifiant $f\mathcal{R}g$ et $g\mathcal{R}h$. On a alors :

$$\forall x \in X \ , \ f(x) \leqslant g(x) \quad \text{et} \quad \forall x \in X \ , \ g(x) \leqslant h(x)$$

La relation $\leqslant$ étant une relation d'ordre sur $\mathbb{R}$, elle est en particulier transitive. Par suite,

$$\forall x \in X \ , \ f(x) \leqslant h(x) \quad \text{c'est-à-dire} \quad f\mathcal{R}h$$

Ce qui prouve que $\mathcal{R}$ est transitive.

Ainsi, $\mathcal{R}$ est bien une relation d'ordre sur $\mathcal{F}(X,\mathbb{R})$. ⊠

Exercice 2.1.2.4 Soit E un ensemble. Montrer que $(\mathcal{P}(E),\subset)$ est un ensemble ordonné.

⚠ **Attention :** le résultat de cet exercice est à connaître : c'est un ensemble ordonné de référence.

2.1.2.a Ordre total et ordre partiel

Définition 2.1.2.5 Soit $(E, \mathcal{R})$ un ensemble ordonné. On dit que $\mathcal{R}$ est un ordre total sur E (ou que $(E, \mathcal{R})$ est totalement ordonné) si deux éléments quelconques de E peuvent toujours être comparés. Autrement dit, $(E, \mathcal{R})$ est totalement ordonné si :

$$\forall (x, y) \in E^2 \ , \ x\mathcal{R}y \text{ ou } y\mathcal{R}x$$

Dans le cas contraire, on dit que $\mathcal{R}$ est un ordre partiel sur E ou que $(E, \mathcal{R})$ est un ensemble partiellement ordonné.

Exemple 2.1.2.6 $(\mathbb{N}, \leqslant)$, $(\mathbb{Z}, \leqslant)$ et $(\mathbb{R}, \leqslant)$ sont des ensembles totalement ordonnés.

Exemple 2.1.2.7 On a déjà vu que $(\mathbb{N}, |)$ est partiellement ordonné.

Exemple 2.1.2.8 De même, si X contient au moins deux éléments, alors $(\mathcal{F}(X, \mathbb{R}), \leqslant)$ est partiellement ordonné. « Intuitivement », c'est évident puisque si l'on prend deux fonctions, la courbe de l'une n'est pas toujours située au-dessus de l'autre. Donnons alors un exemple. Soient a et b deux éléments distincts de X et considérons $f = \delta_a$ et $g = \delta_b$, c'est-à-dire :

$$\begin{array}{rcl} f : X & \longrightarrow & \mathbb{R} \\ x & \longmapsto & \begin{cases} 1 & \text{si } x = a \\ 0 & \text{sinon} \end{cases} \end{array} \quad \text{et} \quad \begin{array}{rcl} g : X & \longrightarrow & \mathbb{R} \\ x & \longmapsto & \begin{cases} 1 & \text{si } x = b \\ 0 & \text{sinon} \end{cases} \end{array}$$

On a alors $f(a) > g(a)$ donc $\exists x \in X \ , \ f(x) > g(x)$, c'est-à-dire $f \leqslant g$ est fausse. De même, $g \leqslant f$ est fausse. Ceci prouve que $\leqslant$ est un ordre partiel sur $\mathcal{F}(X, \mathbb{R})$.

Exercice 2.1.2.9 On considère les relations $\mathcal{R}_1$ et $\mathcal{R}_2$ sur $\mathbb{N}^2$ définies par : pour tout $(p, q) \in \mathbb{N}^2$ et tout $(p', q') \in \mathbb{N}^2$,

$$\begin{array}{rcl} (p, q)\mathcal{R}_1(p', q') & \iff & (p \leqslant p' \text{ et } q \leqslant q') \\ (p, q)\mathcal{R}_2(p', q') & \iff & (p < p' \text{ ou } (p = p' \text{ et } q \leqslant q')) \end{array}$$

1. La relation $\mathcal{R}_1$ est-elle une relation d'ordre ? Est-elle une relation d'ordre totale ?
2. Montrer que $\mathcal{R}_2$ est une relation d'ordre ? Est-elle une relation d'ordre totale ?
3. La relation $\mathcal{R}_2$ est appelée l'ordre lexicographique sur $\mathbb{N}^2$: pourquoi ?

2.1.2.b Majorant, minorant, plus grand et plus petit élément

Définition 2.1.2.10 Soient $(E, \leqslant)$ un ensemble ordonné et A une partie de E.

- Soit $M \in E$. On dit que M est un majorant de A (ou encore M majore A) si :
$$\forall a \in A \ , \ a \leqslant M$$
- On dit que A est majorée (dans E) s'il existe $M \in E$ tel que M majore A.
- Soit $m \in E$. On dit que m est un minorant de A (ou minore A) si
$$\forall a \in A \ , \ m \leqslant a$$
- On dit que A est minorée (dans E) s'il existe $m \in E$ tel que m minore A
- Soit $M \in E$. On dit que M est le plus grand élément de A lorsque M majore A et $M \in A$. Dans ce cas, on note $M = \max A$.
- Soit $m \in E$. On dit que m est le plus petit élément de A lorsque m minore A et $m \in A$. Dans ce cas, on note $m = \min A$.

Proposition 2.1.2.11 *Les définitions du plus petit et plus grand éléments ont un sens : s'il existe, le plus grand élément (respectivement le plus petit élément) est unique.*

Preuve :

Montrons par exemple que si A admet un plus grand élément, alors il est unique. Soient M et M' deux plus grands éléments de A. Par définition :

$$M \in A \text{ et } \forall a \in A \ , \ a \leqslant M \quad (1)$$

et

$$M' \in A \text{ et } \forall a \in A \ , \ a \leqslant M' \quad (2)$$

Puisque $M' \in A$, en choisissant $a = M'$ dans (1), on obtient $M' \leqslant M$. De la même façon, en choisissant $a = M$ dans (2), on obtient $M \leqslant M'$.

Ainsi, on a montré que $M \leqslant M'$ et $M' \leqslant M$. Or, $(E, \leqslant)$ est un ensemble ordonné donc la relation $\leqslant$ est antisymétrique. Par suite, $M = M'$.

$\boxtimes$

Exemple 2.1.2.12 Soient $E = \mathbb{R}$ muni de la relation $\leqslant$ usuelle, $A = [1, 2]$ et $B = [1, 2[$.

- A admet un plus grand élément et $\max A = 2$. En effet,

$$2 \in A \text{ et } \forall x \in A \ , \ x \leqslant 2$$

- En revanche, B n'admet pas de plus grand élément : montrons le par l'absurde. Supposons que B admette un plus grand élément b_0. Alors $b_0 \in B$ et b_0 majore B. Considérons l'élément $b = \dfrac{b_0 + 2}{2}$. Puisque $b_0 \in B$, c'est-à-dire $1 \leqslant b_0 < 2$, il est clair que $b \in B$ et que de plus, $b > b_0$. Ceci contredit le fait que b_0 majore B.

Exemple 2.1.2.13 Soit $E = \mathcal{F}([0, 1], \mathbb{R})$ muni de la relation $\leqslant$ (voir proposition 2.1.2.3). Soient f et g dans E définies pour tout $x \in [0, 1]$ par $f(x) = x$ et $g(x) = 1 - x$. On peut définir la fonction $\max(f, g)$ [1] mais si $A = \{f, g\} \subset E$, alors $\max A$ n'existe pas car :

∗ il existe $x = 0 \in [0, 1]$ tel que $g(x) > f(x)$ (donc $g \leqslant f$ est fausse) ;
∗ il existe $x = 1 \in [0, 1]$ tel que $f(x) > g(x)$ (donc $f \leqslant g$ est aussi fausse).

Exercice 2.1.2.14 On considère l'ensemble ordonné $(\mathbb{N}, |)$ ainsi que les ensembles :

$$A = \{2, 3\} \ ; \ B = \emptyset \ ; \ C = \mathbb{N}^\star$$

Les ensembles A, B et C sont-ils minorés ? Majorés ? Ont-ils un plus grand élément ? Ont-ils un plus petit élément ?

Exemple 2.1.2.15 Soient E un ensemble et $H \in \mathcal{P}(E)$. On définit la relation $\leqslant$ sur $\mathcal{P}(E)$ par :

$$\forall A, B \in \mathcal{P}(E) \ , \ A \leqslant B \iff \begin{cases} A \cap H \subset B \cap H \\ B \cap \overline{H} \subset A \cap \overline{H} \end{cases}$$

où $\overline{H}$ désigne le complémentaire de H dans E.

• Montrons pour commencer que $(\mathcal{P}(E), \leqslant)$ est un ensemble ordonné.

∗ Montrons que $\leqslant$ est réflexive.

Soit $A \in \mathcal{P}(E)$. Il est clair que $A \cap H \subset A \cap H$ et $A \cap \overline{H} \subset A \cap \overline{H}$, c'est-à-dire que $A \leqslant A$. Par suite, $\leqslant$ est bien réflexive.

1. voir chapitre 6, paragraphe 1 : généralités sur les fonctions d'une variable réelle

∗ Montrons que $\leqslant$ est antisymétrique.

Soient A et B deux éléments de $\mathcal{P}(E)$ tels que : $A \leqslant B$ et $B \leqslant A$. Par hypothèse, on a donc :

$$\begin{cases} A \cap H \subset B \cap H \\ B \cap \overline{H} \subset A \cap \overline{H} \end{cases} \quad \text{et} \quad \begin{cases} B \cap H \subset A \cap H \\ A \cap \overline{H} \subset B \cap \overline{H} \end{cases}$$

On en déduit donc, par double inclusion, que :

$$\begin{cases} A \cap H = B \cap H \\ B \cap \overline{H} = A \cap \overline{H} \end{cases}$$

Il s'ensuit que :

$$A = A \cap E = A \cap (H \cup \overline{H}) = (A \cap H) \cup (A \cap \overline{H}) = (B \cap H) \cup (B \cap \overline{H}) = B \cap (H \cup \overline{H}) = B$$

Par conséquent, $A = B$ et la relation $\leqslant$ est antisymétrique.

∗ Montrons que $\leqslant$ est transitive.

Soient $A, B, C \in \mathcal{P}(E)$, trois parties de E telles que $A \leqslant B$ et $B \leqslant C$. Par définition, on a donc :

$$\begin{cases} A \cap H \subset B \cap H \\ B \cap \overline{H} \subset A \cap \overline{H} \end{cases} \quad \text{et} \quad \begin{cases} B \cap H \subset C \cap H \\ C \cap \overline{H} \subset B \cap \overline{H} \end{cases}$$

La relation d'inclusion étant transitive sur $\mathcal{P}(E)$, on a alors :

$$A \cap H \subset B \cap H \text{ et } B \cap H \subset C \cap H \quad \text{entraînent que } A \cap H \subset C \cap H$$

De la même façon, $C \cap \overline{H} \subset B \cap \overline{H} \subset A \cap \overline{H}$. Ainsi :

$$\begin{cases} A \cap H \subset C \cap H \\ C \cap \overline{H} \subset A \cap \overline{H} \end{cases}$$

c'est-à-dire $A \leqslant C$, prouvant ainsi que $\leqslant$ est transitive.

Ce qui prouve que la relation $\leqslant$ est bien une relation d'ordre sur $\mathcal{P}(E)$.

• Montrons que $\mathcal{P}(E)$ admet un plus grand et un plus petit élément (pour $\leqslant$).

∗ Analyse

Supposons que $\mathcal{P}(E)$ admette un plus grand élément X (respectivement un plus petit élément Y). Alors, en particulier, X est un majorant de $\mathcal{P}(E)$ (respectivement Y est un minorant de $\mathcal{P}(E)$). Par conséquent,

$$\forall A \in \mathcal{P}(E)\ ,\ A \leqslant X \quad \text{et} \quad \forall B \in \mathcal{P}(E)\ ,\ Y \leqslant B$$

c'est-à-dire , compte-tenu de la définition,

$$\forall A \in \mathcal{P}(E)\ ,\ \begin{cases} A \cap H \subset X \cap H \\ X \cap \overline{H} \subset A \cap \overline{H} \end{cases} \quad \text{et} \quad \forall B \in \mathcal{P}(E)\ ,\ \begin{cases} Y \cap H \subset B \cap H \\ B \cap \overline{H} \subset Y \cap \overline{H} \end{cases}$$

Les dernières relations étant vraies pour toutes parties A et B de E, on choisit successivement $A = \emptyset = B$ et $A = E = B$, on obtient :

$$\left\{ \begin{array}{rcl} X \cap \overline{H} & = & \emptyset \\ Y \cap H & = & \emptyset \end{array} \right. \quad \text{et} \quad \left\{ \begin{array}{rcl} H & \subset & X \cap H \subset H \\ \overline{H} & \subset & Y \cap \overline{H} \subset \overline{H} \end{array} \right.$$

soit encore,

$$\left\{ \begin{array}{l} X \cap \overline{H} = \emptyset \\ X \cap H = H \end{array} \right. \quad \text{et} \quad \left\{ \begin{array}{l} Y \cap H = \emptyset \\ Y \cap \overline{H} = \overline{H} \end{array} \right.$$

Or,

$$\left\{ \begin{array}{l} X \cap \overline{H} = \emptyset \\ X \cap H = H \end{array} \right. \iff \left\{ \begin{array}{l} X \subset H \\ H \subset X \end{array} \right. \iff X = H$$

Et de la même façon, $Y = \overline{H}$.

∗ Synthèse

Réciproquement, H et $\overline{H}$ sont bien des éléments de $\mathcal{P}(E)$ et de plus,

$$\forall A \in \mathcal{P}(E)\ , \left\{ \begin{array}{l} A \cap H \subset H = H \cap H \\ H \cap \overline{H} = \emptyset \subset A \cap \overline{H} \end{array} \right. \quad \text{c'est-à-dire} \quad \forall A \in \mathcal{P}(E)\ , A \leqslant H$$

On montre de la même façon que pour tout $B \in \mathcal{P}(E)$, $\overline{H} \leqslant B$.

Ce qui prouve que H est le plus grand élément de $\mathcal{P}(E)$ pour la relation $\leqslant$ et que $\overline{H}$ est le plus petit élément de $\mathcal{P}(E)$ pour $\leqslant$.

Remarque : *dans cet exemple, on peut se passer de l'analyse. En effet, on peut deviner très « facilement » que H est le plus grand élément et que $\overline{H}$ est le plus petit élément. Vous pouviez donc simplement rédiger la partie « synthèse » et montrer directement le résultat.*

2.1.2.c Borne supérieure et borne inférieure

Si on reprend l'exemple $B = [1, 2[$, on a vu que B n'a pas de plus grand élément. Pourtant, le « 2 ressemble à une sorte de plus grand élément » : c'est ce qu'on appellera borne supérieure de B et c'est ce qui nous amène à poser les définitions suivantes.

Les notions de bornes supérieure et inférieure, en particulier dans $(\mathbb{R}, \leqslant)$, sont absolument essentielles en analyse. Elles seront entres autres reprises de façon intensive dans le chapitre sur les suites et les limites de fonctions, et sont à la base des théorèmes de limite monotone.

Définition 2.1.2.16 Soient $(E, \leqslant)$ un ensemble ordonné et A une partie de E.

- On dit que A admet une borne supérieure (dans E) si l'ensemble des majorants de A admet un plus petit élément.
  Dans ce cas, ce plus petit élément est appelé la borne supérieure de A et est noté $\sup A$.
- On dit que A admet une borne inférieure (dans E) si l'ensemble des minorants de A admet un plus grand élément.
  Dans ce cas, ce plus grand élément est appelé la borne inférieure de A et est noté $\inf A$.

Remarque : *ainsi, sous réserve d'existence, on peut écrire :*

$$\sup A = \min\{M \in E \mid \forall a \in A\ ,\ a \leqslant M\} \quad et \quad \inf A = \max\{m \in E \mid \forall a \in A\ ,\ m \leqslant a\}$$

On retient donc que si la borne supérieure de A existe, elle est caractérisée par :

$$\forall a \in A\ ,\ a \leqslant \sup A \quad et \quad \forall M \in E\ ,\ ((\forall a \in A\ ,\ a \leqslant M) \Longrightarrow \sup A \leqslant M)$$

Exemple 2.1.2.17 Reprenons $B = [1, 2[$. Intuitivement, il est « évident » que $\sup B = 2$: montrons-le. Notons $\mathrm{Maj}(B)$ l'ensemble des majorants de B. On veut donc prouver que $\min \mathrm{Maj}(B)$ existe et est égal à 2.

- Tout d'abord, $\forall x \in B\ ,\ x \leqslant 2$. Par suite, $2 \in \mathrm{Maj}(B)$.
- Ensuite, soit M un majorant de B. Alors, pour tout $x \in [1, 2[$, $x \leqslant M$. Ceci implique $2 \leqslant M$ (en effet, si $M < 2$, on construit : $b = \frac{M+2}{2} \in B$ vérifiant $M < b$, ce qui contredit le fait que M majore B). Par suite,

$$\forall M \in \mathrm{Maj}(B)\ ,\ 2 \leqslant M$$

Ceci montre que 2 est un minorant de $\mathrm{Maj}(B)$ et appartient à $\mathrm{Maj}(B)$, c'est-à-dire que 2 est le plus petit élément de $\mathrm{Maj}(B)$, c'est-à-dire $2 = \sup B$.

Exercice 2.1.2.18 On considère l'ensemble ordonné $(\mathbb{N}, |)$ et $A = \mathbb{N}^\star \subset \mathbb{N}$. L'ensemble A admet-il un plus grand élément ? Un plus petit élément ? Une borne supérieure ? Une borne inférieure ?

⚠ **Attention :** un ensemble n'a pas forcément de plus grand et/ou de plus petit élément et n'a pas non plus forcément de borne supérieure et/ou inférieure.

Exercice 2.1.2.19 On considère l'ensemble $\mathbb{Q}$ des nombres rationnels muni de la relation $\leqslant$ usuelle et $A = \{x \in \mathbb{Q} \ / \ 0 \leqslant x \text{ et } 0 < x^2 < 2\}$. Montrer que A une borne inférieure (mais pas de plus petit élément) mais que A n'admet pas de borne supérieure.

Proposition 2.1.2.20 *Soit $(E, \leqslant)$ un ensemble ordonné et soit A une partie de E.*

(i) Si A admet un plus grand élément, alors A admet une borne supérieure et :

$$\max A = \sup A$$

(ii) Si A admet un plus petit élément, alors A admet une borne inférieure et :

$$\inf A = \min A$$

Les réciproques des propriétés (i) et (ii) sont fausses.

Preuve :

Ces propriétés sont évidentes. La preuve est laissée en exercice.

⊠

2.1.2.d Applications croissantes, décroissantes et monotones

Définition 2.1.2.21 Soient $(A, \mathcal{R})$ et $(B, \mathcal{S})$ deux ensembles ordonnés et $f : A \longrightarrow B$ une application. On dit que :

- f est croissante si : $\forall (a, a') \in A^2 \ , \ a\mathcal{R}a' \Longrightarrow f(a)\mathcal{S}f(a')$;
- f est strictement croissante si :

$$\forall (a, a') \in A^2 \ , \ (a\mathcal{R}a' \text{ et } a \neq a') \Longrightarrow (f(a)\mathcal{S}f(a') \text{ et } f(a) \neq f(a'))$$

- f est décroissante si : $\forall a, a' \in A \ , \ a\mathcal{R}a' \Longrightarrow f(a')\mathcal{S}f(a)$;
- f est strictement décroissante si :

$$\forall (a, a') \in A^2 \ , \ (a\mathcal{R}a' \text{ et } a \neq a') \Longrightarrow (f(a')\mathcal{S}f(a) \text{ et } f(a) \neq f(a'))$$

- f est monotone si f est croissante ou si f est décroissante ;
- f est strictement monotone si f est strictement croissante ou si f est strictement décroissante.

Exemple 2.1.2.22 L'application identité de $(\mathbb{R}, \leqslant)$ dans lui-même (pour la relation d'ordre usuelle dans $\mathbb{R}$) est strictement croissante.

Exemple 2.1.2.23 L'application $\varphi : (\mathcal{F}(\mathbb{R}, \mathbb{R}), \leqslant) \longrightarrow (\mathbb{R}, \leqslant)$ définie par :

$$\forall f \in \mathcal{F}(\mathbb{R}, \mathbb{R}) \ , \ \varphi(f) = f(0)$$

est croissante mais non strictement croissante. En effet,

- soit $(f, g) \in \mathcal{F}(\mathbb{R}, \mathbb{R})^2$ tel que $f \leqslant g$. Alors, par définition, pour tout réel x, $f(x) \leqslant g(x)$. En particulier, $f(0) \leqslant g(0)$, c'est-à-dire $\varphi(f) \leqslant \varphi(g)$;
- mais si on choisit $f = 0$ (fonction nulle) et $g : x \longmapsto x^2$, alors $f \leqslant g$ et $f \neq g$ mais $\varphi(f) = \varphi(g)$.

Proposition 2.1.2.24 *On considère $(A, \mathcal{R})$ et $(B, \mathcal{S})$ deux ensembles ordonnés ainsi qu'une application $f : A \longrightarrow B$.*

(i) Si f est croissante et injective, alors f est strictement croissante.

(ii) Si f est décroissante et injective, alors f est strictement décroissante.

Preuve :

Montrons par exemple la propriété (i).

On suppose que f est croissante et injective. Soient $a \in A$ et $a' \in A$ deux éléments tels que $a\mathcal{R}a'$ et $a \neq a'$. Puisque f est croissante, $f(a)\mathcal{S}f(a')$ et puisque f est injective (et $a \neq a'$), $f(a) \neq f(a')$. Ce qui prouve que f est strictement croissante.

⊠

Exercice 2.1.2.25 Soit E un ensemble fini non vide. On considère l'application :

$$f : \begin{array}{ccc} (\mathcal{P}(E), \subset) & \longrightarrow & (\mathbb{N}, \leqslant) \\ A & \longmapsto & |A| \end{array}$$

On rappelle que si A est un ensemble fini, $|A|$ désigne le cardinal de l'ensemble A.

1. Montrer que f est strictement croissante.
2. f est-elle injective ?
3. Que peut-on en déduire pour la réciproque de la proposition précédente ?
4. Quelle condition suffisante peut-on rajouter (sur les ensembles ordonnés) pour que cette réciproque soit vraie ?

2.1.3 Relation d'équivalence

Définition 2.1.3.1 Soient E un ensemble et $\mathcal{R}$ une relation binaire sur E. On dit que $\mathcal{R}$ est une relation d'équivalence sur E si $\mathcal{R}$ est réflexive, symétrique et transitive.

⚠ **Attention :** il ne faut absolument pas confondre relation d'ordre et relation d'équivalence !

Exemple 2.1.3.2 La relation d'égalité sur un ensemble quelconque est une relation d'équivalence.

Exemple 2.1.3.3 On a déjà vu que la relation $\parallel$ est une relation d'équivalence sur l'ensemble des droites du plan (voir exemple 2.1.1.4).

Exemple 2.1.3.4 Soit $a \in \mathbb{N}^\star$. Alors la relation de congruence modula a, notée $\equiv [a]$, définie sur $\mathbb{Z}$ par :

$$\forall (x,y) \in \mathbb{Z}^2 \ , \ x \equiv y \ \ [a] \iff a|(y-x)$$

est une relation d'équivalence sur $\mathbb{Z}$ (voir le cours d'arithmétique (proposition 5.1.1.4)).

Exemple 2.1.3.5 Dans les cours de mathématiques antérieurs, on a défini de façon informelle la relation $f \underset{a}{\sim} g$ (on reverra cette définition de façon plus formelle dans le chapitre sur les fonctions d'une variable réelle (voir paragraphe 6.3 du chapitre 6). Alors, la relation $\underset{a}{\sim}$ est une relation d'équivalence sur l'ensemble des fonctions définies sur $\mathbb{R}$.

Exercice 2.1.3.6 Soit $f : \mathbb{R} \longrightarrow \mathbb{R}$ une application. Montrer que la relation $\mathcal{R}$ définie par : $\forall (x,y) \in \mathbb{R}^2 \ , \ x\mathcal{R}y \iff f(x) = f(y)$ est une relation d'équivalence sur $\mathbb{R}$.

Remarque : *d'un point de vue mathématique, les relations d'équivalences sont absolument fondamentales et permettent de définir une des structures les plus importantes : les structures quotients (qui permettent par exemple les constructions très propres et rigoureuses de $\mathbb{Z}$, $\mathbb{Q}$ et $\mathbb{R}$ à partir de $\mathbb{N}$) qui interviennent dans tous les domaines des mathématiques. Mais ceci dépasse de loin l'objectif de ce livre. On se limite ici à la définition et savoir reconnaître une relation d'équivalence.*

2.2 Ensemble $\mathbb{N}$ et principe de récurrence

2.2.1 Définition de l'ensemble $\mathbb{N}$

Théorème 2.2.1.1 (Ensemble $\mathbb{N}$) *On* **admet** *l'existence et l'unicité (à une bijection croissante près) de l'ensemble $\mathbb{N}$, appelé ensemble des entiers naturels, qui est tel que :*

(A1) $\mathbb{N}$ est non vide et est muni d'une relation binaire $\leqslant$ telle que $(\mathbb{N}, \leqslant)$ est un ensemble ordonné ;

(A2) $\mathbb{N}$ est non majoré ;

(A3) toute partie non vide de $\mathbb{N}$ admet un plus petit élément ;

(A4) toute partie non vide et majorée admet un plus grand élément.

De plus, $\mathbb{N}$ est muni de deux lois de composition internes, $+$ et $\times$, qui sont compatibles avec la relation $\leqslant$ et qui vérifient :

- *$+$ et $\times$ sont associatives et commutatives ;*
- *$\times$ est distributive par rapport à $+$;*
- *$+$ admet un élément neutre, noté 0 ;*
- $\forall n \in \mathbb{N}\ ,\ \forall (x,y) \in \mathbb{N}^2\ ,\ x+n \leqslant y+n \Longrightarrow x \leqslant y$;
- $\forall n \in \mathbb{N}\ ,\ \forall (x,y) \in \mathbb{N}^2\ ,\ x+n = y+n \Longrightarrow x = y$;
- *$\times$ admet un élément neutre, noté 1 ;*
- $\forall n \in \mathbb{N}\ ,\ \forall (x,y) \in \mathbb{N}^2\ ,\ (n \times x \leqslant n \times y \ \text{ et } n \neq 0) \Longrightarrow x \leqslant y$;
- $\forall n \in \mathbb{N}\ ,\ \forall (x,y) \in \mathbb{N}^2\ ,\ (n \times x = n \times y \ \text{ et } n \neq 0) \Longrightarrow x = y$.

Remarque : *en fait, seuls les 4 premiers axiomes sont nécessaires. On pourrait définir :*

- $0 = \min \mathbb{N}$ *(puisque $\mathbb{N}$ est non vide (axiome A1) et toute partie non vide de $\mathbb{N}$ admet un plus petit élément (axiome A3) ;*
- $n+1$ *par la relation $n+1 = \min\{p \in \mathbb{N},\ n < p\}$. En effet, comme $\mathbb{N}$ n'est pas majoré (axiome A2), l'ensemble $\{p \in \mathbb{N}\ ,\ n < p\}$ n'est pas vide. Il admet donc un plus petit élément.*
- *si $n \neq 0$, $n-1$ par la relation $n-1 = \max\{p \in \mathbb{N} \mid p < n\}$. En effet, si $n \neq 0$, alors l'ensemble $\{p \in \mathbb{N} \mid p < n\}$ contient $0 = \min \mathbb{N}$ donc est non vide et est majoré par n : il admet donc un plus grand élément (axiome A4).*

Ensuite, avec beaucoup de travail et le principe de récurrence, on définit l'addition, puis la multiplication dans $\mathbb{N}$ et on montre qu'elles vérifient les propriétés énoncées. C'est un travail technique et c'est pour cela qu'on admet leur existence ainsi que leurs propriétés.

Corollaire 2.2.1.2 *À partir des propriétés de $\mathbb{N}$, on déduit immédiatement que :*

(i) $(\mathbb{N}, \leqslant)$ *est un ensemble totalement ordonné, c'est-à-dire :*

$$\forall (a,b) \in \mathbb{N}^2 \ , \ (a \leqslant b \quad ou \quad b \leqslant a)$$

(ii) $\mathbb{N}$ *n'a pas de plus grand élément.*

Preuve :

• Pour la première propriété, soient $a, b \in \mathbb{N}$. Alors $A = \{a, b\}$ est une partie non vide de $\mathbb{N}$: elle admet un plus petit élément. Si $a = \min A$, alors $a \leqslant b$ et sinon, $b = \min A$ et donc $b \leqslant a$. Ceci prouve que $(\mathbb{N}, \leqslant)$ est totalement ordonné.

• Pour la seconde propriété, $\mathbb{N}$ n'étant pas majoré, il ne peut admettre de plus grand élément.

⊠

Notation : si n et p sont deux entiers naturels, on pose :

$$[\![n, p]\!] = \{k \in \mathbb{N} \mid n \leqslant k \leqslant p\}$$

et on convient que si $n > p$, alors $[\![n, p]\!] = \emptyset$.

2.2.2 Principe de récurrence

2.2.2.a Récurrence simple

Théorème 2.2.2.1 *Soit P un prédicat sur $\mathbb{N}$, c'est-à-dire que $P(n)$ est une proposition dépendant du paramètre entier n. Les énoncés suivants sont équivalents :*

(i) $\forall n \in \mathbb{N} \ , \ P(n)$ *;*

(ii) $P(0)$ *et* $\forall n \in \mathbb{N} \ , \ (P(n) \Longrightarrow P(n+1))$.

On dit que (ii) est la preuve de (i) par récurrence.

Preuve :

• Montrons $(i) \Longrightarrow (ii)$.

On suppose (i), c'est-à-dire $\forall n \in \mathbb{N} \ , \ P(n)$. En particulier, pour $n = 0$, on a $P(0)$.

Soit $n \in \mathbb{N}$ fixé. D'après (i), $P(n)$ et $P(n+1)$ sont des propriétés qui sont vraies : on en déduit que l'implication $P(n) \Longrightarrow P(n+1)$ est vraie (d'après la signification du symbole « implique »). Ce qui montre que pour tout $n \in \mathbb{N}$, $P(n) \Longrightarrow P(n+1)$. Ainsi, la propriété (ii) est vraie.

• Montrons $(ii) \Longrightarrow (i)$.
On suppose (ii). Considérons l'ensemble A suivant :

$$A = \{n \in \mathbb{N} \mid \rceil P(n)\} = \{n \in \mathbb{N} \mid P(n) \text{ est faux } \}$$

Alors $A \subset \mathbb{N}$ et la propriété (i) équivaut à montrer que $A = \emptyset$, ce que l'on montre par l'absurde.
Supposons $A \neq \emptyset$. Alors A est une partie non vide de $\mathbb{N}$: elle admet un plus petit élément. Soit $n_0 = \min A$. Puisque $P(0)$ (est vraie), $0 \notin A$ et par conséquent, $n_0 \neq 0$. Ainsi, $k = n_0 - 1 \in \mathbb{N}$ existe et par définition de n_0, $k \notin A$, c'est-à-dire $P(k)$ est vraie. D'après (ii), on a alors $P(k+1)$ est vraie, c'est-à-dire $P(n_0)$ est vraie. Il s'ensuit que $n_0 \notin A$, ce qui est absurde.

$\boxtimes$

Remarque : *en fait, si on reprend la démonstration en détail, on a seulement besoin de l'existence de $n_0 - 1$, et non pas forcément de l'axiome $(A4)$.*

Rappel : pour la rédaction d'une récurrence simple, il y a quatre étapes à rédiger :

1. Introduction : on annonce précisément quelle propriété $P(n)$ on va démontrer par récurrence.
2. Initialisation : on montre que la propriété est vraie au rang 0.
3. Hérédité : on montre que si la propriété est vraie pour un certain entier n, alors elle est vraie pour l'entier $n+1$. En général, pour l'hérédité, on écrit toujours « *on suppose que la propriété $P(n)$ est vraie pour un rang $n \in \mathbb{N}$ donné. Montrons qu'elle est vraie au rang $n+1$* ».
4. Conclusion : on écrit toujours une phrase de conclusion pour dire que le raisonnement par récurrence est terminé.

Exemple 2.2.2.2 Grand classique que vous devez connaître : $\displaystyle\sum_{k=0}^{n} k^2 = \frac{n(n+1)(2n+1)}{6}$.

Montrons par récurrence (simple) que : $\forall n \in \mathbb{N}$, $\displaystyle\sum_{k=0}^{n} k^2 = \frac{n(n+1)(2n+1)}{6}$.

Initialisation :

Pour $n = 0$, on a : $\sum_{k=0}^{n} k^2 = \sum_{k=0}^{0} k^2 = 0 = \frac{n(n+1)(2n+1)}{6}$. Ce qui montre que la propriété est vraie au rang 0.

Hérédité :

On suppose la propriété vraie au rang $n \in \mathbb{N}$: montrons qu'elle est vraie au rang $n+1$. On a :

$$\begin{aligned}
\sum_{k=0}^{n+1} k^2 &= \sum_{k=0}^{n} k^2 + (n+1)^2 \\
&= \frac{n(n+1)(2n+1)}{6} + (n+1)^2 \quad \text{(par hypothèse de récurrence)} \\
&= \frac{(n+1)\left(n(2n+1)+6(n+1)\right)}{6} \\
&= \frac{(n+1)(n+2)(2n+3)}{6} \\
&= \frac{(n+1)(n+2)(2(n+1)+1)}{6}
\end{aligned}$$

Ce qui montre que la propriété est vraie au rang $n+1$ et achève la récurrence.

Conclusion : on a donc montré par récurrence que : $\forall n \in \mathbb{N}$, $\sum_{k=0}^{n} k^2 = \frac{n(n+1)(2n+1)}{6}$.

On peut aussi être amené à faire une récurrence « à partir d'un certain rang » :

Proposition 2.2.2.3 *Soit $n_0 \in \mathbb{N}$ et $P(n)$ une proposition qui dépend du paramètre $n \in \mathbb{N}$. Alors les énoncés suivants sont équivalents :*

(i) $\forall n \geqslant n_0$, $P(n)$;

(ii) $P(n_0)$ *et* $\forall n \geqslant n_0$, $(P(n) \Longrightarrow P(n+1))$.

Preuve :

Il suffit d'appliquer le principe de récurrence à $Q(n) = P(n + n_0)$.

⊠

2.2.2.b Récurrence double

Dans certains cas, on ne peut pas démontrer une propriété par récurrence « simple » dans la mesure où, par exemple, on a une relation de récurrence reliant n, $n+1$ et $n+2$. C'est le cas pour l'exemple suivant.

Exemple 2.2.2.4 On considère la suite $(u_n)_{n\in\mathbb{N}}$ définie par $u_0 = 4$, $u_1 = 5$ et pour tout entier n, $u_{n+2} = 3u_{n+1} - 2u_n$. On veut montrer que pour tout entier n, $u_n = 2^n + 3$. Une récurrence simple ne permet pas de conclure car pour déterminer u_{n+2}, on doit connaître u_n et u_{n+1}.

On utilise alors une récurrence double.

Théorème 2.2.2.5 *Soient P un prédicat sur $\mathbb{N}$ et $n_0 \in \mathbb{N}$. Alors, les énoncés suivants sont équivalents :*

(i) $\forall n \geqslant n_0$, $P(n)$;

(ii) $P(n_0)$ *et* $P(n_0+1)$ *et* $\forall n \geqslant n_0$, $\big((P(n) \text{ et } P(n+1)) \Longrightarrow P(n+2)\big)$.

Preuve :

La démonstration est évidente : il suffit d'appliquer le théorème de récurrence simple à la propriété $Q(n) := P(n) \wedge P(n+1)$, en remarquant que si

$$S \text{ est la propriété : } ((P(n) \wedge P(n+1)) \Longrightarrow P(n+2))$$

alors

$$S \equiv (P(n) \wedge P(n+1)) \Longrightarrow (P(n+1) \wedge P(n+2))$$

⊠

⚠ **Attention :** dans une récurrence double, l'étape d'initialisation comporte deux propriétés !
Il faut montrer que la propriété est vraie aux rangs n_0 et $n_0 + 1$!

Exemple 2.2.2.6 Reprenons l'exemple précédent. On considère la suite $(u_n)_{n\in\mathbb{N}}$ définie par $u_0 = 4$, $u_1 = 5$ et pour tout entier n, $u_{n+2} = 3u_{n+1} - 2u_n$. Montrons par récurrence double que pour tout entier n, $u_n = 2^n + 3$.

Initialisation :

Pour $n = 0$, $u_0 = 4 = 1 + 3 = 2^0 + 3$ et pour $n = 1$, $u_1 = 5 = 2 + 3 = 2^1 + 3$. La propriété est donc vraie aux rangs 0 et 1.

Hérédité :

On suppose la propriété vraie aux rangs n et $n+1$ pour un certain entier n. Montrons qu'elle est vraie au rang $n+2$. On a :

$$\begin{aligned} u_{n+2} &= 3u_{n+1} - 2u_n && \text{(par définition de la suite)} \\ &= 3 \times (2^{n+1} + 3) - 2 \times (2^n + 3) && \text{(hypothèses de récurrence)} \\ &= 4 \times 2^n + 9 - 6 \\ &= 2^{n+2} + 3 \end{aligned}$$

Ce qui montre que la propriété est vraie au rang $n+2$ et achève la récurrence.

Remarque : *on peut bien entendu généraliser ce principe à des récurrences triples, quadruples... ou plus généralement, des récurrences d'ordre $p \in \mathbb{N}^\star$ fixé de la façon suivante. On a équivalence entre :*

(i) $\forall n \in \mathbb{N}$, $P(n)$;

(ii) $\forall k \in [\![0, p-1]\!]$, $P(k)$ *et* $\forall n \in \mathbb{N}$, $\Big(\big(\forall k \in [\![0, p-1]\!]$, $P(n+k)\big) \Longrightarrow P(n+p)\Big)$.

2.2.2.c Récurrence forte

Théorème 2.2.2.7 (Récurrence forte) *Soit P un prédicat sur $\mathbb{N}$. Alors les énoncés suivants sont équivalents :*

(i) $\forall n \in \mathbb{N}$, $P(n)$;

(ii) $P(0)$ *et* $\forall n \in \mathbb{N}$, $\Big(\big(\forall k \in [\![0, n]\!]$, $P(k)\big) \Longrightarrow P(n+1)\Big)$.

Preuve :

À nouveau, ce théorème est une conséquence directe de la récurrence simple. Il suffit pour cela d'appliquer le théorème de récurrence simple à $Q(n) := \forall k \in [\![0, n]\!]$, $P(k)$ et de remarquer, comme pour la récurrence double, qu'en notant S la propriété :

$$(\forall k \in [\![0, n]\!] \text{ , } P(k)) \Longrightarrow P(n+1)$$

alors

$$S \equiv (\forall k \in [\![0, n]\!] \text{ , } P(k)) \Longrightarrow (\forall k \in [\![0, n+1]\!] \text{ , } P(k))$$

⊠

Exemple 2.2.2.8 Montrons par récurrence forte que tout entier naturel supérieur ou égal à 2 s'écrit comme un produit de facteurs premiers.

Initialisation :

Au rang $n = 2$, on a $2 = 2$ qui est bien un produit de facteurs premiers (en fait, il y a un seul facteur). La propriété est vraie au rang 2.

Hérédité :

Soit $n \in \mathbb{N}$ tel que $n \geqslant 2$. On suppose que tout entier $k \in [\![2, n]\!]$ se décompose en facteurs premiers. Montrons qu'il en est de même pour $n+1$. On a alors deux cas :

- si $n+1$ est premier, alors $n+1 = (n+1)$ est un produit de nombres premiers (produit ayant un seul facteur) ;
- sinon, $n+1$ est composé : il existe $a, b \in \mathbb{N}$ tels que $n+1 = ab$ et $a \neq 1$ et $a \neq n+1$. Il s'ensuit que $b \neq 1$ et $b \neq n+1$. Par suite, $a, b \in [\![2, n]\!]$. On applique alors l'hypothèse à a et à b : a et b s'écrivent comme un produit de nombres premiers. Par conséquent, $n+1 = a \times b$ s'écrit lui aussi comme un produit de nombres premiers.

Ceci montre que la propriété est vraie au rang $n+1$ et achève la récurrence.

Exercice 2.2.2.9 Soit $(u_n)_{n\in\mathbb{N}}$ définie par $u_0 \in \mathbb{R}$ et $\forall n \in \mathbb{N}$, $u_{n+1} = \sum_{k=0}^{n} u_k$.
Montrer que pour tout entier $n \in \mathbb{N}$, $u_{n+1} = u_0 \times 2^n$.

2.2.2.d Récurrence finie et récurrence descendante

Dans certaines situations, on est amené à prouver qu'une propriété est vraie, mais seulement pour certains entiers. Typiquement, pour un nombre fini d'entiers. On dispose alors des deux théorèmes suivants.

Théorème 2.2.2.10 (Récurrence finie) *Soient $n \in \mathbb{N}$ et P un prédicat sur $[\![0, n]\!]$ (ou sur $\mathbb{N}$). Alors les énoncés suivants sont équivalents :*

(i) $\forall k \in [\![0, n]\!]$, $P(k)$;

(ii) $P(0)$ *et* $\forall k \in [\![0, n-1]\!]$, $(P(k) \Longrightarrow P(k+1))$.

Preuve :

Remarquez que si $n = 0$, il n'y a rien à prouver car $[\![0, n[\![= \emptyset$ et dans ce cas, la propriété, $\forall k \in [\![0, n[\![$, $(P(k) \Longrightarrow P(k+1))$ est automatiquement vraie.
Lorsque $n \geqslant 1$, on peut faire exactement la même démonstration que pour la récurrence simple. ⊠

Bien entendu, on peut aussi faire un raisonnement par récurrence double finie ou récurrence forte finie.

Exemple 2.2.2.11 Soient $n \in \mathbb{N}^\star$ et f une bijection de $[\![0, n]\!]$ dans lui-même telle que pour tout $k \in [\![0, n]\!]$, $f(k) \leq k$.
Montrons par récurrence forte finie que pour tout $k \in [\![0, n]\!]$, $f(k) = k$.

Initialisation :

Par hypothèse, d'une part $f(0) \in [\![0, n]\!]$ donc $0 \leqslant f(0)$ et d'autre part $f(0) \leqslant 0$. Par suite, $f(0) = 0$ et la propriété est vraie au rang $k = 0$.

Hérédité :

Soit $k \in \mathbb{N}$ et $k < n$. On suppose que la propriété est vraie jusqu'au rang k. Montrons qu'elle est vraie au rang $k+1$. D'après l'hypothèse de récurrence, $\forall j \in [\![0, k]\!]$, $f(j) = j$. Alors :

- d'une part, $f(k+1) \in [\![0, n]\!] \setminus \{f(j)\ ,\ 0 \leqslant j \leqslant k\}$ (car f est injective et $k+1 \neq j$ pour tout $j \in [\![0, k]\!]$), c'est-à-dire $f(k+1) \geqslant k+1$;
- et d'autre part, d'après l'hypothèse sur f, $f(k+1) \leqslant k+1$.

Il s'ensuit que $f(k+1) = k+1$, ce qui montre que la propriété est vraie au rang $k+1$ et achève la récurrence.

Remarque : *on verra dans le cours d'arithmétique que l'algorithme d'Euclide se prouve par récurrence finie.*

Théorème 2.2.2.12 (Récurrence descendante) *Soient $n \in \mathbb{N}$ et P un prédicat sur $[\![0, n]\!]$ (ou sur $\mathbb{N}$). Les énoncés suivants sont équivalents :*

(i) $\forall k \in [\![0, n]\!]$, $P(k)$;

(ii) $P(n)$ *et* $\forall k \in [\![1, n]\!]$, $(P(k) \Longrightarrow P(k-1))$.

Preuve :

Il suffit d'appliquer le théorème de récurrence finie à $Q(k) := P(n-k)$.

⊠

Exercice 2.2.2.13 Soient $n \in \mathbb{N}^\star$ et f une bijection de $[\![0, n]\!]$ dans lui-même telle que pour tout $k \in [\![0, n]\!]$, $f(k) \geqslant k$. Montrer que pour tout $k \in [\![0, n]\!]$, $f(k) = k$.

2.3 Ensemble $\mathbb{Z}$ et valeur absolue

2.3.1 Ensemble $\mathbb{Z}$ et structure d'anneau

Théorème 2.3.1.1 (Admis) *On admet l'existence de l'ensemble $\mathbb{Z}$, appelé ensemble des entiers relatifs, et des opérations $+$ et $\times$ qui en font un anneau commutatif et intègre. L'ensemble $\mathbb{Z}$ contient $\mathbb{N}$, et les lois $+$ et $\times$ de $\mathbb{Z}$ prolongent celles de $\mathbb{N}$.*

Par ailleurs, $\mathbb{Z}$ est muni d'une relation d'ordre $\leqslant$, prolongeant celle de $\mathbb{N}$, et telle que :

- *l'ordre est compatible avec l'addition ;*
- $\mathbb{N} = \{z \in \mathbb{Z} \mid 0 \leqslant z\}$ *et* $\mathbb{Z} = \mathbb{N} \cup \{-n \ , \ n \in \mathbb{N}^\star\}$.

Remarques et conséquences immédiates :

• On sait que dans $\mathbb{N}$, la multiplication est compatible avec l'ordre. Puisque les opérations sur $\mathbb{Z}$ prolongent celles de $\mathbb{N}$, on en déduit que :

$$\forall x, y \in \mathbb{Z} \ , \ (0 \leqslant x \text{ et } 0 \leqslant y) \Longrightarrow 0 \leqslant xy$$

- On en déduit que pour tout $(a, b) \in \mathbb{Z}^2$ et $n \in \mathbb{N}$, $a \leqslant b \Longrightarrow na \leqslant nb$.
- Enfin, comme $\leqslant$ est compatible avec $+$, $\{-n \ , \ n \in \mathbb{N}^\star\} = \{z \in \mathbb{Z} \mid z < 0\}$.

Théorème 2.3.1.2 (Existence d'un minimum et d'un maximum) *On a :*

(i) Toute partie non vide et minorée de $\mathbb{Z}$ admet un plus petit élément.

(ii) Toute partie non vide et majorée de $\mathbb{Z}$ admet un plus grand élément.

Preuve :

(i) Soit A une partie non vide et minorée de $\mathbb{Z}$ et soit $m \in \mathbb{Z}$ un minorant. Considérons alors $A' = \{a - m \ , \ a \in A\}$. Par construction, A' est une partie non vide de $\mathbb{N}$: elle admet donc un plus petit élément. Soit x ce plus petit élément. Alors $x + m$ est le plus petit élément de A.

(ii) Soit A une partie non vide et majorée de $\mathbb{Z}$. Alors l'ensemble B défini par $B = -A = \{-a \ , \ a \in A\}$ est une partie non vide et minorée de $\mathbb{Z}$. D'après (i), elle admet un plus petit élément x. Il est alors clair que $-x$ est le plus grand élément de A.

⊠

Corollaire 2.3.1.3 $(\mathbb{Z}, \leqslant)$ *est un ensemble totalement ordonné.*

Preuve :

Soient $a, b \in \mathbb{Z}$. Alors $A = \{a, b\}$ est une partie non vide de $\mathbb{Z}$. On distingue alors trois cas :

- si $a, b \in \mathbb{N}$, alors A est non vide et minorée (par 0) donc admet un plus petit élément ;
- si $a, b \in \mathbb{Z} \setminus \mathbb{N}$, alors A est une partie non vide et majorée (par 0) de $\mathbb{Z}$ donc A admet un plus grand élément ;
- enfin, si $a < 0$ et $0 \leqslant b$ (ou le contraire), alors $b = \max A$ (respectivement $a = \max A$).

⊠

Corollaire 2.3.1.4 *Soit $A \subset \mathbb{Z}$. Alors :*

$$A \text{ est un ensemble fini} \iff A \text{ est majoré et minoré}$$

Preuve :

On considère les ensembles $A_1 = A \cap \mathbb{N}$, $A_2 = A \cap \mathbb{Z}^{\star -} = \{a \in A \mid a < 0\}$ et $B = -A_2 = \{-a \ , \ a \in A_2\} \subset \mathbb{N}$. Tout d'abord, $A = A_1 \sqcup A_2$. Par conséquent, A est fini si et seulement si A_1 et A_2 le sont.

Ensuite, clairement, A_2 et B sont en bijection donc A_2 est fini si et seulement si B l'est.

Enfin, on peut montrer qu'une partie de $\mathbb{N}$ est finie si et seulement si elle est majorée. On a alors :

$$\begin{aligned} A \text{ est fini} &\iff A_1 \text{ et } A_2 \text{ sont finis} \\ &\iff A_1 \text{ et } B \text{ sont finis} \\ &\iff A_1 \text{ et } B \text{ sont majorés} \\ &\iff A_1 \text{ est majoré et } A_2 \text{ est minoré} \\ &\iff A \text{ est majoré et minoré} \end{aligned}$$

⊠

Remarque : $\mathbb{Z}$ *est un anneau intègre, c'est-à-dire que :*

$$\forall x, y \in \mathbb{Z} \ , \ (xy = 0 \Longrightarrow x = 0 \ \textit{ou} \ y = 0)$$

2.3.2 Valeur absolue dans $\mathbb{Z}$

Définition 2.3.2.1 Soit $x \in \mathbb{Z}$. On appelle valeur absolue de x, et on note $|x|$, l'unique entier naturel dans $\{-x, x\}$.

Remarque : *de façon équivalente,* $|x| = \max\{-x, x\}$. *Ainsi, pour tout* $x \in \mathbb{Z}$, $|-x| = |x|$ *et* $|x| = 0 \iff x = 0$.

Proposition 2.3.2.2 *Pour tout* $(x, y) \in \mathbb{Z}^2$, $|x \times y| = |x| \times |y|$.

Preuve :

Il suffit de distinguer les cas possibles suivant les signes de x et y, on verra une preuve similaire un peu plus loin dans le cas l'ensemble $\mathbb{R}$. ⊠

2.4 Ensembles des nombres réels

2.4.1 Corps des nombres rationnels

Définition 2.4.1.1 On note $\mathbb{Q}$ l'ensemble des nombres rationnels :

$$\mathbb{Q} = \left\{ \frac{p}{q} \ , \ (p, q) \in \mathbb{Z} \times \mathbb{N}^* \right\}$$

On admet le résultat suivant, que l'on a déjà partiellement vu dans le chapitre sur les structures.

Théorème 2.4.1.2 *L'ensemble* $(\mathbb{Q}, +, \times)$ *est un corps commutatif. De plus,* $(\mathbb{Q}, \leq)$ *est totalement ordonné.*

Remarque : *cette définition n'est pas satisfaisante dans la mesure où on n'a pas défini* $\frac{1}{q}$ *pour* $q \in \mathbb{Z}^\star$. *La construction formelle de* $\mathbb{Q}$ *est proche de celle de* $\mathbb{Z}$ *(voir annexe) mais ne sera pas présentée. Pour ceux qui sont intéressés, vous pouvez consulter n'importe quelle ouvrage d'algèbre qui aborde la notion de corps des fractions d'un anneau intègre.*

2.4.2 Corps des nombres réels et relation d'ordre

On admet le théorème fondamental suivant.

Théorème 2.4.2.1 (Définition) *Il existe un ensemble noté $\mathbb{R}$ (appelé ensemble des nombres réels) contenant $\mathbb{Q}$, muni d'une addition $+$, d'une multiplication $\times$ et d'une relation d'ordre $\leqslant$ tels que :*

- *les lois $+$ et $\times$ sur $\mathbb{R}$ prolongent celles de $\mathbb{Q}$;*
- *$(\mathbb{R}, +, \times)$ est un corps commutatif ;*
- *la relation $\leqslant$ sur $\mathbb{R}$ prolonge celle de $\mathbb{Q}$ et $(\mathbb{R}, \leqslant)$ est totalement ordonné ;*
- *la relation d'ordre est compatible avec l'addition et la multiplication :*

$$\forall (x, y, z) \in \mathbb{R}^3 \ , \ (x \leqslant y \Longrightarrow x + z \leqslant y + z)$$

$$\forall (x, y) \in \mathbb{R}^2 \ , \ ((0 \leqslant x \text{ et } 0 \leqslant y) \Longrightarrow 0 \leqslant xy)$$

- *$(\mathbb{R}, \leqslant)$ vérifie le théorème de la borne supérieure : toute partie non vide et majorée de $\mathbb{R}$ admet une borne supérieure.*

2.4.3 Valeur absolue

Définition 2.4.3.1 Pour tout réel x, on pose $|x| = \max\{-x, x\}$.

Remarque : *en particulier, $x \leqslant |x|$ pour tout réel x.*

Proposition 2.4.3.2 *L'ensemble $\mathbb{R}^{+\star} = \{x \in \mathbb{R} \ , \ 0 < x\}$ est un sous-groupe de $(\mathbb{R}^\star, \times)$. De plus, la valeur absolue est un morphisme de groupes de $(\mathbb{R}^\star, \times)$ dans $(\mathbb{R}^{+\star}, \times)$. Autrement dit,*

$$\forall x, y \in \mathbb{R}^\star \ , \ |x \times y| = |x| \times |y|$$

(la dernière égalité étant aussi valable lorsque $x = 0$ ou $y = 0$).
En particulier, si $x \neq 0$, alors : $\left|\dfrac{1}{x}\right| = \dfrac{1}{|x|}$.

Preuve :

• Montrons d'abord que $(\mathbb{R}^{+\star}, \times)$ est un sous-groupe de $(\mathbb{R}^{\star}, \times)$. Pour commencer, on peut noter que comme $(\mathbb{R}, +, \times)$ est un corps, $(\mathbb{R}^{\star}, \times)$ est bien un groupe. On applique ensuite la méthode habituelle :

- $0 < 1$ donc $1 \in \mathbb{R}^{+\star}$;
- soient $x > 0$ et $y > 0$. $\mathbb{R}$ étant un corps, *a fortiori* c'est un anneau intègre donc $xy \neq 0$. Par ailleurs, d'après la définition de $\mathbb{R}$, la multiplication est compatible avec la relation d'ordre : $0 \leqslant x$ et $0 \leqslant y$ impliquent $0 \leqslant xy$. Par suite, $0 < xy$ et $xy \in \mathbb{R}^{+\star}$;
- enfin, soit $x \in \mathbb{R}^{+\star}$. $(\mathbb{R}, \leqslant)$ étant totalement ordonné, $0 \leqslant x^{-1}$ ou bien $x^{-1} \leqslant 0$. Par ailleurs, x^{-1} étant non nul, $x^{-1} < 0$ ou bien $0 < x^{-1}$. Si $x^{-1} < 0$, alors $(-x^{-1}) + x^{-1} < 0 + (-x^{-1})$, c'est-à-dire $0 < -x^{-1}$. Il s'ensuit que $0 < x \times (-x^{-1})$. D'après les règles de calculs dans un anneau, $0 < -1$, c'est-à-dire $1 < 0$ ce qui est absurde. Par suite, $0 < x^{-1}$.

Ainsi, $(\mathbb{R}^{+\star}, \times)$ est un sous-groupe de $(\mathbb{R}^{\star}, \times)$.

• Montrons à présent que la valeur absolue est un morphisme de groupes, de $(\mathbb{R}^{\star}, \times)$ dans $(\mathbb{R}^{+\star}, \times)$.

Le même raisonnement que pour l'inverse de x montre que dans $\mathbb{R}$, on a la règle des signes : si $0 < x$ et $0 < y$, alors $0 < xy$; si $x < 0$ et $0 < y$, alors $xy < 0$ et si $x < 0$ et $y < 0$, alors $0 < xy$.
Soient alors $x, y \in \mathbb{R}^{\star}$. On distingue deux cas :

- Premier cas : x et y ont le même signe.
  Si $0 < x$ et $0 < y$, alors $0 < xy$ et donc $|x| = x$, $|y| = y$ et $|xy| = xy = |x| \times |y|$.
  Si $x < 0$ et $y < 0$, alors $0 < xy$ et on a $|x| = -x$, $|y| = -y$ et $|xy| = xy$. Par suite, $|xy| = xy = (-x) \times (-y) = |x| \times |y|$.
- Deuxième cas : x et y sont de signes contraires.

  Dans ce cas, quitte à échanger les noms, on peut supposer $0 < x$ et $y < 0$. Dans ce cas, $|x| = x$ et $|y| = -y$ et $xy < 0$. Par suite, $|xy| = -(x \times y) = x \times (-y) = |x| \times |y|$.

Ce qui montre que $\forall x, y \in \mathbb{R}^{\star}$, $|xy| = |x| \times |y|$. On remarque d'ailleurs que cette relation est encore valable si $x = 0$ ou $y = 0$.

• Enfin, soit $x \in \mathbb{R}^{\star}$: alors $x \times x^{-1} = 1$. D'après ce qui précède, on a alors :

$$|x \times x^{-1}| = |1| \quad \text{c'est-à-dire} \quad |x| \times |x^{-1}| = 1$$

Sachant que $|x| \neq 0$, on obtient : $|x^{-1}| = |x|^{-1}$.

⊠

Remarque : *vous aurez bien remarqué que la preuve de la dernière propriété est inutile ! C'est une propriété des morphismes de groupes.*

Proposition 2.4.3.3 (Inégalité triangulaire) *Pour tous $x, y \in \mathbb{R}$, $|x+y| \leqslant |x|+|y|$. De plus, il y a égalité si et seulement si $0 \leqslant xy$, c'est-à-dire si et seulement si x et y ont le même signe (au sens large).*

Preuve :

• Montrons d'abord l'inégalité.

Par définition de la valeur absolue, on a d'une part $x \leqslant |x|$ et $y \leqslant |y|$ donc $x + y \leqslant |x| + |y|$; et d'autre part, $-x \leqslant |x|$ et $-y \leqslant |y|$ donc $-(x + y) \leqslant |x| + |y|$.

Par suite, $|x + y| = \max\{(x + y), -(x + y)\} \leqslant |x| + |y|$.

• Traitons à présent le cas d'égalité.

∗ Si $|x + y| = |x| + |y|$, alors : $(x + y)^2 = |x + y|^2 = (|x| + |y|)^2$, c'est-à-dire $xy = |xy|$. Par suite, $0 \leqslant xy$, c'est-à-dire x et y ont le même signe (au sens large).

∗ Réciproquement, supposons que x et y aient le même signe (au sens large). On distingue alors deux cas :

- si $x = 0$ ou $y = 0$, alors il est clair que $|x + y| = |x| + |y|$;
- sinon, $0 < xy$, et il y a alors deux possibilités :
  · soit $0 < x$ et $0 < y$ et donc $0 < x + y$. On en déduit donc que $|x + y| = x + y = |x| + |y|$;
  · ou bien $x < 0$ et $y < 0$ et dans ce cas, $x + y < 0$. Alors $|x + y| = -(x + y) = -x - y = |x| + |y|$.

⊠

Interprétation : *$|x - y|$ est la distance entre deux points. Si $a, b, c \in \mathbb{R}$, $x = b - a$, $y = c - b$ alors $x + y = c - a$ et l'inégalité triangulaire s'écrit $|c - a| \leqslant |b - a| + |c - b|$.*

Corollaire 2.4.3.4 *Soient x et y deux réels. Alors :*

$$\big|\, |x| - |y| \,\big| \leqslant |x - y| \leqslant |x| + |y|$$

La démonstration est laissée en exercice.

2.4.4 Propriétés de la borne supérieure et de la borne inférieure

Pour commencer, on rappelle les définitions suivantes :

Définition 2.4.4.1 Soit $(E, \leqslant)$ un ensemble ordonné et soit $A \subset E$. On dit que A admet une borne supérieure si l'ensemble des majorants de A (dans E) admet un plus petit élément. On pose alors :

$$\sup A = \min\{M \in E \ , \ M \text{ majore A}\} = \min\{M \in E \ / \ \forall a \in A \ , \ a \leqslant M\}$$

De façon similaire, on dit que A admet une borne inférieure dans E si l'ensemble des minorants de A (dans E) admet un plus grand élément. On pose alors :

$$\inf A = \max\{m \in E \ , \ m \text{ minore } A\} = \max\{m \in E \ / \ \forall a \in A \ , \ m \leqslant a\}$$

Remarque : *au début de ce chapitre, on a vu que :*

- *si A admet un plus grand élément, alors dans ce cas, A admet une borne supérieure et* $\max A = \sup A$ *;*
- *par contre la réciproque est fausse. Par exemple,* $[0, 1[$ *admet une borne supérieure qui est* 1 *mais pas de plus grand élément.*

Par définition de l'ensemble $\mathbb{R}$ des nombres réels vérifie la propriété de la borne supérieure, c'est-à-dire :

Théorème 2.4.4.2 (ADMIS) *Toute partie non vide et majorée de $\mathbb{R}$ admet une borne supérieure.*

Remarque : *ce théorème est un théorème essentiel, on l'utilisera à de très nombreuses reprises : pour les suites et le théorème de la limite monotone (qui permet par exemple de prouver que $\mathbb{R}$ est complet (voir cours de mathématiques spéciales 1), pour le théorème des valeurs intermédiaires et bien d'autres fois).*

On en déduit immédiatement que $\mathbb{R}$ vérifie la propriété de la borne inférieure :

Corollaire 2.4.4.3 *Toute partie non vide et minorée de $\mathbb{R}$ admet une borne inférieure.*

Preuve :

Soit A une partie non vide et minorée de $\mathbb{R}$. Considérons alors l'ensemble :

$$B = -A = \{-a \ , \ a \in A\}$$

Il est clair que B est une partie non vide et majorée de $\mathbb{R}$: elle admet donc une borne supérieure. Montrons alors que $\inf A = -\sup(B)$.

• Montrons que $-\sup(B)$ minore A.
Soit $x \in A$, alors $-x \in B$: par suite, $-x \leqslant \sup(B)$ et donc $-\sup(B) \leqslant x$. Ceci étant vrai pour tout $x \in A$, $-\sup(B)$ est un minorant de A.

• Montrons que $-\sup(B)$ majore tout minorant de A.
Soit m un minorant de A (il existe par hypothèse sur A). Alors, $-m$ est un majorant de $-A$, c'est-à-dire $-m$ est un majorant de B. Par définition de la borne supérieure, on a donc $\sup(B) \leqslant -m$. Par suite, $m \leqslant -\sup(B)$.

On a donc démontré que $-\sup(B)$ est un minorant de A et que tout minorant de A lui est inférieur ou égal. Par conséquent, $-\sup(-A)$ est le plus grand des minorants de A, c'est-à-dire A admet une borne inférieure qui est $\inf(A) = -\sup(B) = -\sup(-A)$.

⊠

Exemple 2.4.4.4 Soient A et B deux parties non vides et majorés de $\mathbb{R}$. On note :

$$C = \{x \in \mathbb{R} \ / \ \exists (a,b) \in A \times B \ , \ x = a + b\}$$

(l'ensemble C est usuellement noté $C = A+B$). Montrons que $\sup(C) = \sup(A)+\sup(B)$.

• On commence par justifier l'existence des bornes supérieures !

- A (respectivement B) est une partie non vide et majorée de $\mathbb{R}$. Par conséquent A (respectivement B) admet une borne supérieure.
- C est une partie de $\mathbb{R}$ et $C \neq \emptyset$ car A et B sont non vides. De plus, soit $c \in C$. Alors, par définition, il existe $(a,b) \in A \times B$ tel que $c = a + b$. On en déduit que :

$$c = a + b \leqslant \sup A + \sup B$$

Ceci montre que C est également majorée et donc, C admet une borne supérieure.

• D'après ce qui précède, $\sup A + \sup B$ est un majorant de C. Par conséquent,

$$\sup C \leqslant \sup A + \sup B$$

Réciproquement, soit $a \in A$. Alors, pour tout $b \in B$, $(a + b) \in C$ et donc $a + b \leqslant \sup(C)$, soit encore $b \leqslant c - a \leqslant \sup(C) - a$. Ce qui montre que $\sup C - a$ est un majorant de B et ainsi, par définition de la borne supérieure :

$$\sup(B) \leqslant \sup(C) - a$$

Ainsi, pour tout $a \in A$, $a \leqslant \sup(C) - \sup(B)$. Par conséquent, $\sup(A) \leqslant \sup(C) - \sup(B)$, c'est-à-dire :

$$\sup(A) + \sup(B) \leqslant \sup(C)$$

Il s'ensuit que $\sup(C) = \sup(A) + \sup(B)$.

Remarque : *de façon générale, montrer qu'un ensemble admet une borne supérieure est assez difficile et c'est encore plus difficile de déterminer cette borne supérieure. Dans le cas des parties de $\mathbb{R}$, l'existence est « facile » car on dispose de la propriété de la borne supérieure. En revanche, déterminer la valeur de cette borne supérieure est en général assez difficile.*

La proposition suivante est essentielle. Elle permet de caractériser la borne supérieure dans $\mathbb{R}$. C'est cette caractérisation qui sera presque toujours utilisée.

Proposition 2.4.4.5 (Caractérisation de la borne supérieure dans $\mathbb{R}$) *Soit A une partie non vide et majorée de $\mathbb{R}$. Les propriétés suivantes sont équivalentes :*

(i) $M = \sup A$ *;*

(ii) M *majore* A *et* $\forall \varepsilon > 0$, $\exists a \in A$, $M - \varepsilon < a \leqslant M$.

Preuve :

• $(i) \Longrightarrow (ii)$

On suppose que $M = \sup(A)$. Alors, par définition, M majore A. De plus, toujours par définition, M est le plus petit des majorants de A. Soit $\varepsilon > 0$: $M - \varepsilon < M$. Par conséquent, $M - \varepsilon$ n'est pas un majorant de A, c'est-à-dire qu'il existe $a \in A$ tel que : $M - \varepsilon < a$. D'où $M - \varepsilon < a \leqslant M$.

• $(ii) \Longrightarrow (i)$

On suppose que M majore A et $(\star)$: $\forall \varepsilon > 0$, $\exists a \in A$, $M - \varepsilon < a \leqslant M$. Montrons que $M = \sup(A)$.
Notons $Maj(A)$ l'ensemble des majorants de A. Par hypothèse, M majore A donc $M \in Maj(A)$. Par ailleurs, si $m \in \mathbb{R}$ vérifie $m < M$, on choisit $\varepsilon = M - m > 0$: d'après la propriété $(\star)$, il existe $a \in A$ tel que : $m < a$. Par conséquent, m n'est pas un majorant de A. Ceci montre que M est un minorant de $Maj(A)$.
Ainsi, on a montré que $M \in Maj(A)$ et $\forall m \in Maj(A)$, $M \leqslant m$. Par conséquent, $M = \sup(A)$.

$\boxtimes$

Corollaire 2.4.4.6 *Soit B une partie non vide et minorée de $\mathbb{R}$. Les propriétés suivantes sont équivalentes :*

(i) $m = \inf(B)$ *;*

(ii) m *minore* B *et* $\forall \varepsilon > 0$, $\exists b \in B$, $m \leqslant b < m + \varepsilon$.

Exemple 2.4.4.7 Soit f une application croissante de $[0,1]$ dans lui-même. On veut montrer que f admet un point fixe, c'est-à-dire qu'il existe $x \in [0,1]$ tel que $f(x) = x$.

Pour cela, on considère l'ensemble $E = \{x \in [0,1] \ , \ x \leqslant f(x)\}$ et on va montrer que $\sup E$ est un point fixe de f.

• Montrons pour commencer que E admet une borne supérieure.

Tout d'abord, $E \subset \mathbb{R}$. De plus, puisque f va de $[0,1]$ dans $[0,1]$, $f(0) \in [0,1]$ et *a fortiori*, $0 \leqslant f(0)$, c'est-à-dire $0 \in E$ et E est donc non vide. De plus, par définition, $E \subset [0,1]$ donc E est majoré (par 1).

Ainsi, E est une partie non vide et majorée de $\mathbb{R}$: elle admet donc une borne supérieure. Soit $a = \sup E$.

• Montrons que $f(a) = a$.

∗ Pour tout $x \in E$, $x \leqslant a$ (puisque a est un majorant de E). Or, f est croissante donc :

$$f(x) \leqslant f(a) \quad \text{et par suite} \quad x \leqslant f(x) \leqslant f(a) \ \ (\text{car } x \in E)$$

Il s'ensuit que $f(a)$ est un majorant de E et donc $\sup(E) \leqslant f(a)$, c'est-à-dire $a \leqslant f(a)$.

∗ D'après ce qui précède, $a \leqslant f(a)$. Or, f est croissante donc $f(a) \leqslant f(f(a))$, c'est-à-dire $f(a) \in E$. Par suite, $f(a) \leqslant \sup E$, c'est-à-dire $f(a) \leqslant a$.

Ce qui prouve que $f(a) = a$.

Remarque : *pour montrer que $a \in E$, on pouvait aussi utiliser la caractérisation de la borne supérieure dans $\mathbb{R}$. En effet, pour $\varepsilon > 0$, il existe $x \in E$ tel que $a - \varepsilon < x \leqslant a$. On en déduit alors que $f(x) \leqslant f(a)$ et comme $x \in E$, $a - \varepsilon < x \leqslant f(x) \leqslant f(a)$. On obtient donc :*

$$\forall \varepsilon > 0 \ , \ a - \varepsilon \leqslant f(a)$$

Ce qui implique que $a \leqslant f(a)$. En effet, si $a > f(a)$, on choisit $\varepsilon = \frac{a-f(a)}{2} > 0$, et on obtient $\frac{a+f(a)}{2} \leqslant f(a)$, soit encore $\frac{a-f(a)}{2} \leqslant 0$ ce qui est absurde.

Exercice 2.4.4.8 Soit A une partie non vide et majorée de $\mathbb{R}$ et soit $f : \mathbb{R} \longrightarrow \mathbb{R}$ une application croissante. Comparer $f(\sup A)$ et $\sup f(A)$ après avoir justifié l'existence de ces nombres. Énoncer puis démontrer un résultat analogue lorsque f est décroissante.

2.4.5 Partie entière

Lemme 2.4.5.1 $\mathbb{N}$ *n'est pas majoré dans* $\mathbb{R}$.

Preuve :

On raisonne par l'absurde et on suppose que $\mathbb{N}$ est majoré dans $\mathbb{R}$.
Alors $\mathbb{N}$ est une partie non vide et majorée de $\mathbb{R}$: elle admet une borne supérieure. Soit $M = \sup \mathbb{N}$.
Par définition, M majore $\mathbb{N}$. Montrons alors que $\dfrac{M}{2}$ majore $\mathbb{N}$ aussi.
Soit $n \in \mathbb{N}$, alors $2n \in \mathbb{N}$ donc $2n \leqslant M$, soit encore $n \leqslant \dfrac{M}{2}$. Comme $M = \sup \mathbb{N}$, et que la borne supérieure est le plus petit des majorants, $M \leqslant \dfrac{M}{2}$, c'est-à-dire $M \leqslant 0$.
Par ailleurs, $1 \in \mathbb{N}$ donc $1 \leqslant M$ (car M majore $\mathbb{N}$). Par suite, $M \leqslant 0$ et $1 \leqslant M$: ce qui est absurde.

⊠

Corollaire 2.4.5.2 $\mathbb{Z}$ *n'est ni majoré, ni minoré dans* $\mathbb{R}$.

Preuve :

C'est clair : c'est une conséquence directe du fait que $\mathbb{N}$ n'est pas majoré dans $\mathbb{R}$.

⊠

Proposition 2.4.5.3 (Définition) *Soit $x \in \mathbb{R}$. Il existe un unique entier $n \in \mathbb{Z}$ tel que :*

$$n \leqslant x < n + 1$$

Cet unique entier relatif n est appelé la partie entière de x et est noté $E(x)$ (ou aussi $[x]$, ou encore $\lfloor x \rfloor$).

Preuve :

Soit $A = \{m \in \mathbb{Z}\ ,\ m \leqslant x\}$. Alors A est une partie non vide (puisque x n'est pas un minorant de $\mathbb{Z}$) et majorée de $\mathbb{Z}$. Par conséquent, A admet un plus grand élément : soit $n = \max A$. Alors, $n \leqslant x$ et par définition, $n+1 \notin A$, c'est-à-dire $n+1 > x$.

⊠

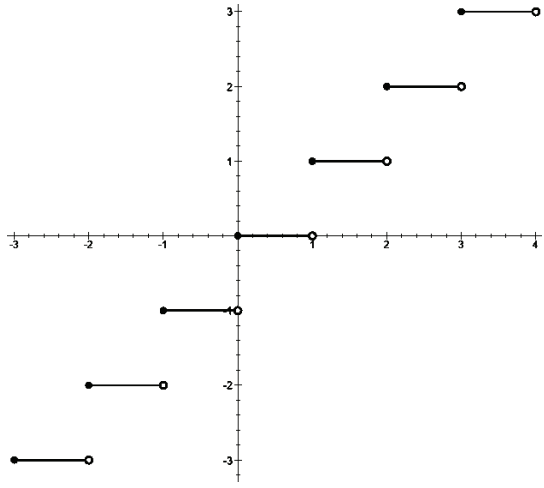
Remarque : *la fonction E est 1-périodique et par définition, pour tout réel x,*

$$E(x) \leqslant x < E(x) + 1$$

Exercice 2.4.5.4 Montrer que $E(x) \underset{x\to+\infty}{\sim} x$ et $E(x) \underset{x\to-\infty}{\sim} x$. Ce résultat est à connaître.

Exercice 2.4.5.5 Quelles sont les parties entières de : $x = 5$, $x = 2,4$, $x = 3,9$ et $x = -1,1$?

Remarque : *voici l'allure de la courbe représentative de la fonction partie entière*



En particulier, cette fonction n'est pas continue sur $\mathbb{R}$ (voir chapitre 6), mais elle l'est sur $\mathbb{R} \setminus \mathbb{Z}$. Plus exactement, elle est discontinue en tout point $n \in \mathbb{Z}$ et :

$$\lim_{\substack{x\to n\\ x<n}} E(x) = n-1 \qquad \lim_{\substack{x\to n\\ x>n}} E(x) = n$$

Exercice 2.4.5.6 Montrer que $\forall (x,y) \in \mathbb{R}^2$, $E(x)+E(y) \leqslant E(x+y) \leqslant E(x)+E(y)+1$ et donner un exemple où chaque inégalité est une égalité.

Proposition 2.4.5.7 (Axiome d'Archimède) *Pour tous $x, y \in \mathbb{R}_+^\star$, il existe $n \in \mathbb{N}$ tel que $x < ny$.*

Preuve :

Posons $n = E\left(\frac{x}{y}\right) + 1$. Alors $\dfrac{x}{y} < n$ et donc $x < ny$ (car $y > 0$). ⊠

2.4.6 Caractérisation des intervalles de $\mathbb{R}$

Définition 2.4.6.1 Soient a, b deux réels tels que $a \leqslant b$. On appelle segment d'extrémités a et b, et on note $[a, b]$, l'ensemble des nombres réels x vérifiant $a \leqslant x \leqslant b$. De même, on pose :

$$\begin{aligned}
]a, b] &= \{x \in \mathbb{R} \mid a < x \leqslant b\} \\
]a, b[&= \{x \in \mathbb{R} \mid a < x < b\} \\
]a, b] &= \{x \in \mathbb{R} \mid a < x \leqslant b\} \\
]-\infty, b] &= \{x \in \mathbb{R} \mid x \leqslant b\} \\
]-\infty, b[&= \{x \in \mathbb{R} \mid x < b\} \\
[a, +\infty[&= \{x \in \mathbb{R} \mid a \leqslant x\} \\
]a, +\infty[&= \{x \in \mathbb{R} \mid a < x\}
\end{aligned}$$

Remarque : *si $b < a$, alors par définition $[a, b] = \emptyset$.*

Définition 2.4.6.2 Soit I une partie de $\mathbb{R}$. On dit que I est un intervalle si :

$$\forall (x, y) \in I^2 \ , \ [x, y] \subset I$$

Remarque : *on reverra plus tard (cours de mathématiques supérieures 2 : fonctions convexes) qu'en fait cette définition est celle d'un ensemble convexe. On va en réalité montrer que les parties convexes de $\mathbb{R}$ sont exactement les intervalles de $\mathbb{R}$, c'est-à-dire les ensembles de la forme de la définition précédente.*

Proposition 2.4.6.3 *Soit $I \subset \mathbb{R}$. Alors I est un intervalle si et seulement si :*

- *il existe $(a,b) \in \mathbb{R}^2$ tel que $I = [a,b]$ ou $I = [a,b[$ ou $I =]a,b]$ ou $I =]a,b[$;*
- *ou il existe $a \in \mathbb{R}$ tel que $I = [a,+\infty[$ ou $I =]a,+\infty[$;*
- *ou il existe $b \in \mathbb{R}$ tel que $I =]-\infty,b]$ ou $I =]-\infty,b[$.*

Preuve :

Ce théorème peut être admis en première lecture. Pour ceux qui sont intéressés, voici une preuve.

• On commence par la réciproque qui est évidente.

Si I est d'une des formes précédentes, alors il est clair que I est un intervalle. En effet, supposons par exemple que $I = [a,b[$ avec $a \leqslant b$ et soient $x, y \in I$ tels que $x < y$. Soit $z \in [x,y]$. Alors, $x \leqslant z \leqslant y$. Or $x \in I$ donc $a \leqslant x$ et de même $y < b$. Par transitivité, $a \leqslant z < y$, c'est-à-dire $z \in I$. On a donc montré que $[x,y] \subset I$ et I est un intervalle.

• Montrons à présent $\Longrightarrow$.

Soit I un intervalle de $\mathbb{R}$. Pour commencer, si I est vide, il suffit de prendre $a = b = 1$ et dans ce cas, $[a,b[= \emptyset = I$.
On suppose maintenant que I est non vide. On distingue alors les quatre cas suivants :

(1) I est majoré et minoré ;

(2) I est minoré et non majoré ;

(3) I est majoré et non minoré ;

(4) I n'est ni majoré, ni minoré.

Premier cas : (1)

I est une partie non vide et majorée (respectivement minorée) de $\mathbb{R}$: elle admet donc une borne supérieure (respectivement inférieure). Posons $a = \inf I$ et $b = \sup I$. I étant non vide, $a \leqslant b$. Il faudrait ici aussi traiter les cas $(a,b) \in I^2$, $a \in I$ et $b \notin I$, $a \notin I$ et $b \in I$, $a \notin I$ et $b \notin I$.
Traitons par exemple le cas $a \in I$ et $b \notin I$. Montrons que $I = [a,b[$.

∗ Montrons l'inclusion $I \subset [a,b[$.
Soit $x \in I$. Alors par définition, $a \leqslant x \leqslant b$. Par ailleurs, comme $b \notin I$ et $x \in I$, $x \neq b$. Par suite, $x \in [a,b[$.

* Montrons à présent que $[a, b[\subset I$.
  Soit $x \in [a, b[$. Si $x = a$, alors $x \in I$ et c'est réglé : on suppose donc $x > a$. Puisque $x < b$, d'après la caractérisation de la borne supérieure dans $\mathbb{R}$, (avec $\varepsilon = \frac{b-x}{2} > 0$ par exemple), il existe $i \in I$ tel que $b - \frac{b-x}{2} < i \leqslant b$. On a alors : $x < i < b$ (puisque $i \neq b$).
  De même, $\exists j \in I$, $a \leqslant j < a + \frac{x-a}{2} < x$. Soit un tel j. On a alors : $x \in [j, i]$ et $j, i \in I$. I étant un intervalle, on en déduit que $x \in I$.

Les autres cas du (1) se traitent de façon similaire.

Deuxième cas : (2)

I est non vide et minoré donc admet une borne inférieure dans $\mathbb{R}$. Posons $a = \inf I$. On distingue deux cas selon que $a \in I$ ou non.
Traitons le cas où $a \notin I$ et montrons alors que $I =]a, +\infty[$.

* L'inclusion $I \subset]a, +\infty[$ est évidente par définition de la borne inférieure (c'est un minorant de I) et du fait qu'on a supposé que $a \notin I$.

* Montrons que $]a, +\infty[\subset I$.
  Soit $x \in]a, +\infty[$. I n'est pas majoré : par suite, x n'est pas un majorant de I. Il existe $i \in I$ tel que $x < i$. Par ailleurs, $a = \inf I$: pour $\varepsilon = \dfrac{x-a}{2}$, il existe $j \in I$ tel que $a \leqslant j < a + \varepsilon < x$.
  Alors, $x \in [j, i] \subset I$.

Troisième cas : (3)

Le cas (3) se déduit en appliquant (2) à l'ensemble $-I$.

Quatrième cas : (4)

Montrons que $I = \mathbb{R}$. L'inclusion $I \subset \mathbb{R}$ étant vérifiée, on doit seulement prouver que $\mathbb{R} \subset I$. Soit $x \in \mathbb{R}$. Alors :

* x ne majore pas I (puisque I n'est pas majoré) : il existe $i \in I$ tel que $x < i$;
* de même, x ne minore pas I : il existe $j \in I$ tel que $j < x$.

On a alors $x \in [j, i] \subset I$, c'est-à-dire $x \in I$. D'où $I = \mathbb{R}$.

⊠

Exercice 2.4.6.4 Soit A un intervalle de $\mathbb{R}$. On suppose qu'il existe $T > 0$ tel que $A + T = A$ (voir exemple 2.2.4.4 pour la définition de $A + T$). Montrer que $A = \mathbb{R}$.

2.4.7 Droite numérique achevée

Définition 2.4.7.1 On appelle droite numérique achevée, et on note $\overline{\mathbb{R}}$, l'ensemble $\mathbb{R} \cup \{-\infty, +\infty\}$, où $+\infty$ et $-\infty$ sont deux symboles, non réels, tels que : $-\infty = \min \overline{\mathbb{R}}$ et $+\infty = \max \overline{\mathbb{R}}$. On a alors :

$$\overline{\mathbb{R}} = [-\infty, +\infty] \quad \text{et} \quad \forall x \in \mathbb{R}\ ,\ -\infty < x < +\infty$$

Remarques :

- *ceci permettra en particulier de parler de limite dans $\overline{\mathbb{R}}$ pour dire qu'une limite existe mais n'est pas nécessairement finie ;*
- *$\overline{\mathbb{R}}$ est muni d'une relation d'ordre $\leqslant$ qui prolonge celle de $\mathbb{R}$ avec la règle donnée dans la définition ;*
- *on peut définir dans $\overline{\mathbb{R}}$ une addition et une multiplication (qui sont commutatives et qui prolongent l'addition et la multiplication dans $\mathbb{R}$) à quelques formes indéterminées près :*

$$\forall a \in \mathbb{R}\ ,\ (+\infty) + a = a + (+\infty) = +\infty \quad ; \quad (-\infty) + a = a + (-\infty) = -\infty$$

On a également :

$$(+\infty) + (+\infty) = +\infty \quad (-\infty) + (-\infty) = -\infty$$

Mais en revanche, l'addition $+\infty + (-\infty)$ n'est pas définie.

Pour la multiplication, la seule forme indéterminée est $0 \times \infty$.

2.4.8 Densité de $\mathbb{Q}$ et de $\mathbb{R} \setminus \mathbb{Q}$

Définition 2.4.8.1 Soit $A \subset \mathbb{R}$, une partie de $\mathbb{R}$. On dit que A est dense dans $\mathbb{R}$ si : $\forall (a, b) \in \mathbb{R}^2\ ,\ (a < b \Longrightarrow A \cap]a, b[\neq \emptyset\ )$.

Remarques :

- *lorsqu'on étudiera les suites réelles, on montrera que cette définition est équivalente à dire que tout nombre réel s'obtient comme limite d'une suite d'éléments de A. C'est la caractérisation séquentielle de la densité (qui est absolument essentielle) ;*

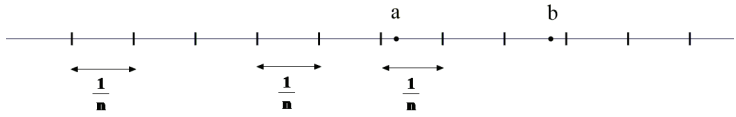
- *la notion de partie dense est très importante en mathématique. Cette définition sera utilisée dans le chapitre sur limite et continuité et sera généralisée dans le chapitre sur les espaces vectoriels normés (cours de mathématiques spéciales 1).*

Théorème 2.4.8.2 *$\mathbb{Q}$ et $\mathbb{R} \setminus \mathbb{Q}$ sont denses dans $\mathbb{R}$.*

Preuve :

• Montrons que $\mathbb{Q}$ est dense dans $\mathbb{R}$.

Soit $(a, b) \in \mathbb{R}^2$ tel que $a < b$. Montrons que $\mathbb{Q} \cap]a, b[\neq \emptyset$. L'idée est très simple, il suffit « de couper $\mathbb{R}$ » en des petits intervalles de longueur constante $\frac{1}{n}$ (avec n entier), mais de longueur suffisamment petite pour qu'on ne puisse pas passer de a à un nombre plus grand que b :



De façon rigoureuse, par définition, $b - a > 0$ et il existe $n \in \mathbb{N}^\star$ tel que $n > \frac{1}{b-a}$ car $\mathbb{N}$ n'est pas majoré (ceci nous donne le découpage « assez petit » voulu). On considère alors l'ensemble :

$$B = \{k \in \mathbb{Z} \ , \ k \leqslant na\}$$

B est une partie non vide (puisque $\mathbb{Z}$ n'est pas minoré) et majorée (par définition de B) de l'ensemble $\mathbb{Z}$. Par conséquent, B admet un plus grand élément. Posons $p = \max(B) + 1$.
Par définition du plus grand élément, $p \notin B$, c'est-à-dire $p > na$ soit encore, $a < \frac{p}{n}$ (puisque $n > 0$). Par ailleurs, $\frac{p}{n} = \frac{p-1}{n} + \frac{1}{n}$. Or, $p - 1 \in B$ donc $\frac{p-1}{n} \leqslant a$ et $\frac{1}{n} < b - a$. En additionnant, il vient : $\frac{p}{n} < b$. Ce qui montre que $\frac{p}{n} \in \mathbb{Q} \cap]a, b[$. D'où le résultat.

• Montrons que $\mathbb{R} \setminus \mathbb{Q}$ est dense dans $\mathbb{R}$.

On applique exactement le même raisonnement à un petit détail près : il existe $n \in \mathbb{N}^\star$ tel que $\frac{\sqrt{2}}{(b-a)} < n$. Puis $B = \{k \in \mathbb{Z} \ , \ k \leqslant \frac{na}{\sqrt{2}}\}$. Le raisonnement est alors identique : on vérifie que si $p = \max B + 1$, alors $\frac{p\sqrt{2}}{n} \in (\mathbb{R} \setminus \mathbb{Q}) \cap]a, b[$.

⊠

Remarque : *dans la remarque précédente, on a parlé de la caractérisation séquentielle de la densité. C'est une méthode encore plus élémentaire pour prouver la densité de* $\mathbb{Q}$ *(et de* $\mathbb{R} \setminus \mathbb{Q}$*) dans* $\mathbb{R}$*. En effet, on a prouvé précédemment que :*

$$\frac{E(x)}{x} \underset{x\to+\infty}{\sim} 1 \quad \textit{c'est-à-dire} \qquad \lim_{x\to+\infty} \frac{E(x)}{x} = 1$$

On a alors pour tout $x \neq 0$ *:*

$$\lim_{n\to+\infty} \frac{E(10^n x)}{10^n} = x \quad \textit{et } \forall n \in \mathbb{N}\ ,\ u_n = \frac{E(10^n x)}{10^n} \in \mathbb{Q}$$

Pour $x = 0$*, il suffit de prendre* $u_n = \dfrac{1}{n}$ *pour tout entier* n*. Dans les deux cas, on obtient une suite de nombres rationnels qui converge vers* x*.*

Pour les irrationnels, si $x \neq 0$*,*

$$\lim_{n\to+\infty} \frac{E(10^n x\sqrt{2})}{10^n\sqrt{2}} = x \quad \textit{et } \forall n \in \mathbb{N}\ ,\ u_n = \frac{E(10^n x\sqrt{2})}{10^n\sqrt{2}} \in \mathbb{R} \setminus \mathbb{Q}$$

Pour $x = 0$*,* $u_n = \dfrac{\sqrt{2}}{n}$ *est une suite de nombre irrationnels qui converge vers* x*.*

Pour terminer ce paragraphe, voici un exercice difficile qui reprend beaucoup de notions différentes et permet de « classifier » les sous-groupes de $\mathbb{R}$.

Exercice 2.4.8.3 Soit G un sous-groupe de $(\mathbb{R}, +)$. On suppose $G \neq \{0\}$.

1. Montrer que l'ensemble $G^+ = G \cap]0, +\infty[$ admet une borne inférieure. On pose par la suite $a = \inf G^+$.
2. On suppose dans cette question uniquement que $a > 0$.
   (a) En raisonnant par l'absurde, démontrer que $a \in G$.
   (b) En déduire que $a\mathbb{Z} \subset G$ puis montrer que $G = a\mathbb{Z}$.
   On rappelle que $a\mathbb{Z} = \{na\ ,\ n \in \mathbb{Z}\}$.
3. On suppose cette fois que $a = 0$. On fixe deux réels x et y tels que $x < y$.
   (a) Justifier qu'il existe $g \in G$ tel que $0 < g < y - x$.
   (b) Montrer que l'ensemble $\{n \in \mathbb{Z} \mid ng \leqslant x\}$ admet un plus grand élément.
   (c) En déduire qu'il existe $h \in G$ tel que $x < h < y$.
   (d) Que vient-on de prouver sur le groupe G ?
4. Énoncer clairement le théorème qui vient d'être démontré sur les sous-groupes de $(\mathbb{R}, +)$.

5. Applications :

   (a) Montrer que pour tout réel x, il existe une suite de nombres de la forme $x_n = a_n + b_n\sqrt{2}$ avec $a_n, b_n \in \mathbb{Z}$ tels que (x_n) converge vers x.

   (b) Montrer que $\mathbb{Z} + 2\pi\mathbb{Z}$ est un sous-groupe de $(\mathbb{R}, +)$. En déduire que l'ensemble $\{\cos(n)\ ,\ n \in \mathbb{N}\}$ est dense dans $[-1, 1]$.

   (c) Généralisation : que peut-on dire de l'ensemble $\alpha\mathbb{Z} + 2\pi\mathbb{Z}$ lorsque $\alpha \in \mathbb{R}$?

   (d) *Attention : cette question suppose connue la notion de continuité.* Soit f une application de $\mathbb{R}$ dans $\mathbb{R}$.

      i. Montrer que l'ensemble $T(f)$ des périodes (positives ou négatives) de f est un sous-groupe de $\mathbb{R}$.

      ii. On suppose que f est continue, périodique et non constante. Montrer qu'il existe un unique $T > 0$ tel que $T(f) = T\mathbb{Z}$ (ce T est appelé la plus petite période de f).

      iii. Donner un exemple de fonction (non continue) pour laquelle $T(f)$ est une partie dense de $\mathbb{R}$.

      iv. On suppose que f est dérivable. Montrer que $T(f) = T(f')$. *On pourra utiliser qu'une fonction continue sur $\mathbb{R}$ et périodique est bornée sur $\mathbb{R}$.*

2.4.9 Valeurs décimales approchées d'un nombre réel

Définition 2.4.9.1 Étant donné $\varepsilon \in \mathbb{R}^{+\star}$, on dit qu'un réel r est une approximation d'un réel x à ε près si $|x - r| \leqslant \varepsilon$. De plus, si $x \leqslant r$, on dit qu'il s'agit d'une approximation par excès et si $r \leqslant x$, r est une approximation par défaut.

Proposition 2.4.9.2 *Soient $x \in \mathbb{R}$ et $n \in \mathbb{N}$. Alors il existe un unique entier relatif $z \in \mathbb{Z}$ tel que :*

$$z \times 10^{-n} \leqslant x < (z+1)10^{-n}$$

$z \times 10^{-n}$ (respectivement $(z+1) \times 10^{-n}$) s'appelle l'approximation décimale par défaut (respectivement par excès) de x à 10^{-n} près.

Preuve :

C'est évident : $z = E\left(10^n x\right)$ est l'unique entier relatif cherché.

⊠

2.5 Exercices

Exercice 2.5.1 Dans $\mathbb{R}$, on considère la relation $\mathcal{R}$ définie par :

$$\forall (x,y) \in \mathbb{R}^2,\ ,\ x\mathcal{R}y \Longleftrightarrow x^2 - y^2 = x - y$$

1. Vérifier que $\mathcal{R}$ est une relation d'équivalence.
2. Pour tout $x \in \mathbb{R}$, on appelle *classe d'équivalence de x modulo $\mathcal{R}$* et on note $cl_{\mathcal{R}}(x)$ l'ensemble :
$$cl_{\mathcal{R}}(x) = \{y \in \mathbb{R} \ / \ x\mathcal{R}y\}$$
Calculer $cl_{\mathcal{R}}(x)$ pour $x \in \mathbb{R}$.

Exercice 2.5.2 On définit une relation binaire $\preceq$ sur $\mathbb{R}^{+\star}$ par :

$$\forall (x,y) \in (\mathbb{R}^{+\star})^2\ ,\ (x \preceq y \Longleftrightarrow \exists n \in \mathbb{N}\ ;\ y = x^n)$$

Montrer que $\preceq$ est une relation d'ordre. Est-elle un ordre total ?

Exercice 2.5.3 On définit une relation binaire $\preceq$ sur $H = \{z \in \mathbb{C} \ / \ \Im m(z) \geq 0\}$ par :

$$\forall (z,z') \in H^2\ ,\ z \preceq z' \Longleftrightarrow \Big(|z| < |z'| \text{ ou } (|z| = |z'| \text{ et } \Re e(z) \leq \Re e(z'))\Big)$$

Montrer qu'il s'agit d'une relation d'ordre total sur H.

Exercice 2.5.4 Soient E un ensemble et $A \subset \mathcal{P}(E)$, c'est-à-dire que A est un sous-ensemble de $\mathcal{P}(E)$.

1. A est-elle une partie majorée, minorée de $(\mathcal{P}(E), \subset)$?
2. A admet-elle nécessairement un plus grand élément ? Un plus petit élément ? Si oui, les déterminer.
3. A admet-elle une borne supérieure ? Si oui, la déterminer.
4. A admet-elle une borne inférieure ? Si oui, la déterminer.

Exercice 2.5.5 Soit f l'application de $\mathbb{R}$ dans $\mathbb{R}$ définie par :

$$f(x) = \begin{cases} \arctan(x) & \text{si } x < -1 \\ \dfrac{\pi}{4}x - \dfrac{\pi}{2} & \text{si } -1 \leqslant x \leqslant 0 \\ \dfrac{\pi}{2}(1 - \operatorname{th}(x)) & \text{si } x > 0 \end{cases}$$

1. Propriétés de la fonction f.
   (a) Déterminer les limites de f aux bornes de son ensemble de définition.
   (b) Étudier la continuité de f sur son ensemble de définition.
   (c) Calculer $f'(x)$ lorsque cela a un sens, puis étudier les variations de la fonction f et tracer sa courbe représentative.
   (d) f est-elle injective ? Surjective ? Bijective ? Justifier la réponse.
   (e) Déterminer $\mathrm{Im} f$ puis $f^{-1}(]-\frac{\pi}{2},\frac{\pi}{2}[)$.
2. On considère la relation binaire $\mathcal{R}$ définie sur $\mathbb{R}\times\mathbb{R}$ par :
$$\forall (x,y)\in\mathbb{R}^2\ ,\ x\mathcal{R}y \iff f(x)\leqslant f(y)$$
   (a) Montrer que $\mathcal{R}$ est une relation d'ordre sur $\mathbb{R}$.
   (b) $(\mathbb{R},\mathcal{R})$ est-il un ensemble totalement ordonné ? Justifier la réponse.
   (c) L'ensemble $\mathbb{R}$ est-il majoré, minoré pour $\mathcal{R}$? Justifier la réponse.

Exercice 2.5.6 Soit G un groupe fini et H un sous-groupe de G.
On définit la relation binaire $\mathcal{R}$ sur l'ensemble G par :
$$\forall (x,y)\in G\ ,\ x\mathcal{R}y \iff x^{-1}y\in H$$
1. Montrer que $\mathcal{R}$ est une relation d'équivalence sur G.
2. Pour $x\in G$, on définit $\mathrm{cl}(x)=\{g\in G\mid x\mathcal{R}g\}$. Montrer que :
$$\forall x,y\in G\ ,\ \mathrm{cl}(x)=\mathrm{cl}(y) \iff x\mathcal{R}y$$
3. Montrer également que :
$$\forall x,y\in G\ ,\ x\ \not\mathcal{R}y \iff \mathrm{cl}(x)\cap\mathrm{cl}(y)=\emptyset$$
4. On considère l'ensemble $X=\{\mathrm{cl}(x)\ ,\ x\in G\}$. Montrer que X est un ensemble fini.
5. On note $X=\{P_1,\cdots,P_n\}$. Montrer que les $(P_i)_{1\leqslant i\leqslant n}$ forment une partition de G, en parties non vides.
6. Montrer que pour tout $i\in[\![1,n]\!]$, P_i est un ensemble fini et $|P_i|=|H|$.
7. En déduire que $|G|=|X|\times|H|$.
8. Que vient-on de démontrer ?

Comparez cet exercice avec l'exercice 1.3.19 dans le chapitre sur les groupes, anneaux et corps.

Exercice 2.5.7 Démontrer que pour tout entier naturel n, $2^n \geqslant n$.

Exercice 2.5.8 Démontrer que pour tout entier n,

$$1 \times 2 + 2 \times 3 + \cdots + (n-1) \times n = \frac{(n-1)n(n+1)}{3}$$

et écrire le produit sous forme symbolique.

Exercice 2.5.9 Démontrer que pour tout entier n,

$$\sum_{k=1}^{n} k^2 = \frac{n(n+1)(2n+1)}{6} \text{ et } \sum_{k=1}^{n} k^3 = \left(\frac{n(n+1)}{2}\right)^2$$

Exercice 2.5.10 Montrer que $\{n \in \mathbb{N} \mid 2^n > n^3\}$ admet un plus petit élément n_0 et le déterminer. Montrer ensuite que pour tout entier $n \geqslant n_0$, $2^n > n^3$.

Exercice 2.5.11 Soit (F_n) la suite de Fibonacci définie par $F_0 = 0$, $F_1 = 1$ et pour tout entier n, $F_{n+2} = F_{n+1} + F_n$. On pose $\phi = \dfrac{1+\sqrt{5}}{2}$ (nombre d'or). Démontrer que pour tout $n \in \mathbb{N}^\star$, $\phi^{n-2} \leqslant F_n \leqslant \phi^{n-1}$.

Exercice 2.5.12 Pour quelles valeurs de n a-t-on l'inégalité : $\dfrac{1}{n^3} < \dfrac{1}{n^2} - \dfrac{1}{(n+1)^2}$? En déduire que $\forall n \in \mathbb{N}^\star$, $1 + \dfrac{1}{2^3} + \dfrac{1}{3^3} + \cdots + \dfrac{1}{n^3} < \dfrac{5}{4}$.

Exercice 2.5.13 Soit $f : \mathbb{N} \longrightarrow \mathbb{N}$ une application injective telle que $\forall n \in \mathbb{N}$, $f(n) \leqslant n$. Montrer que $f = \mathrm{Id}_{\mathbb{N}}$.

Exercice 2.5.14 Soit f une application strictement croissante de $\mathbb{N}$ dans $\mathbb{N}$ vérifiant $f(2) = 2$ et :

$$\forall n, m \in \mathbb{N} \text{ , } f(nm) = f(n) \times f(m)$$

Déterminer les fonctions f possibles.

Exercice 2.5.15 On veut déterminer toutes les applications f de $\mathbb{N}$ dans $\mathbb{N}$ telles que :

$$\forall n \in \mathbb{N} \text{ , } f(f(n)) < f(n+1)$$

1. Montrer par récurrence que pour tout $p \in \mathbb{N}$: $\forall n \geqslant p$, $f(n) \geqslant p$.
2. En déduire que f est croissante puis trouver f.

Exercice 2.5.16 Un étudiant fait le raisonnement suivant :

« *Soit un réel $a > 0$. Alors pour tout entier $n \neq 0$, $a^{n-1} = 1$.*

Preuve par récurrence : le résultat est vrai pour $n = 1$ et s'il est vrai pour $1, 2, \cdots, n$, alors :

$$a^{(n+1)-1} = a^n = \frac{a^{n-1} \times a^{n-1}}{a^{n-2}} = \frac{1 \times 1}{1} = 1$$

Ce qui montre que la propriété est vraie au rang $n+1$ et achève la récurrence ».

Qu'en pensez-vous ?

Exercice 2.5.17 Calculer les sommes suivantes :

$$\sum_{k=1}^{n} k^2(n+1-k) \quad ; \quad \sum_{k=1}^{n} k(k+1) \quad ; \quad \sum_{1 \leqslant i \leqslant j \leqslant n} ij \quad ; \quad \sum_{\substack{1 \leqslant i \leqslant n \\ 1 \leqslant j \leqslant n}} \inf(i,j)$$

Exercice 2.5.18 Calculer les sommes suivantes :

$$\sum_{k=0}^{n} k\binom{n}{k} \quad ; \quad \sum_{k=0}^{n} (-1)^k \binom{n}{k} \quad ; \quad \sum_{k=0}^{n} k^2 \binom{n}{k} \quad ; \quad \sum_{k=0}^{n} \frac{1}{k+1}\binom{n}{k}$$

Exercice 2.5.19 Montrer que pour tout $(n,p) \in \mathbb{N}^2$ tel que $p \leqslant n$, $\displaystyle\sum_{k=p}^{n} \binom{k}{p} = \binom{n+1}{p+1}$.

Exercice 2.5.20 Soient p, q et n trois entiers tels que $n \leqslant p+q$.

1. En calculant de deux façons différentes le coefficient en x^n dans le polynôme $P(x) = (1+x)^p(1+x)^q$, démontrer que :

$$\sum_{k=0}^{n} \binom{p}{k}\binom{q}{n-k} = \binom{p+q}{n}$$

   où l'on pose $\binom{a}{b} = 0$ lorsque $b > a$. En déduire que : $\displaystyle\sum_{k=0}^{p} \binom{p}{k}\binom{q}{n-k} = \binom{p+q}{n}$.

2. Retrouver le résultat précédent en interprétant en terme de dénombrement.
3. Dans quelle loi de probabilité usuelle avez-vous déjà vu cette identité ?

Exercice 2.5.21 Calculer pour $n \in \mathbb{N}^\star$ les nombres suivants :

$$S_1 = \sum_{\substack{1 \leqslant i \leqslant n \\ 1 \leqslant j \leqslant n}} |i-j| \quad ; \quad S_2 = \sum_{i=1}^{n}\sum_{j=i}^{n} \frac{i}{j+1} \quad ; \quad S_3 = \sum_{k=2}^{n} \ln\left(1 - \frac{1}{k}\right) \quad ; \quad S_4 = \prod_{i=1}^{n}\prod_{j=1}^{n} i^j$$

Exercice 2.5.22 Soit $(E, \leqslant)$ un ensemble non vide et ordonné tel que toute partie non vide de E admet un plus petit élément et un plus grand élément.

1. Montrer que $(E, \leqslant)$ est totalement ordonné.
2. On suppose que E est infini.
   (a) Montrer alors qu'on peut construire par récurrence une suite $(u_n)_{n\in\mathbb{N}}$ d'éléments de E telle que (u_n) est strictement croissante.
   (b) On pose $A = \{u_n \ , \ n \in \mathbb{N}\}$. A admet-il un plus grand élément ?
   (c) Conclure.
3. On veut prouver le résultat de la question précédente par une autre méthode. On pose pour $x \in E$, $\left]\leftarrow, x\right] = \{y \in E \ , \ y \leqslant x\}$.
   (a) Soit $A = \{x \in E \ , \ \left]\leftarrow, x\right] \text{ est fini }\}$. Montrer que A admet un plus grand élément.
   (b) Prouver que $E = \left]\leftarrow, \max A\right]$ et en déduire que E est un ensemble fini.

Exercice 2.5.23 Décomposition en base factorielle

1. Montrer que : $\forall n \in \mathbb{N}^\star \ , \ \displaystyle\sum_{k=1}^{n} k \times k! = (n+1)! - 1$.
2. On souhaite maintenant prouver que tout entier $N \in \mathbb{N}^\star$ se décompose de façon unique en :
$$N = \sum_{k=1}^{n} a_k k!$$
où $(\star)$ $n \in \mathbb{N}^\star$, $a_n \neq 0$ et $\forall k \in [\![1, n]\!]$, $a_k \in [\![0, k]\!]$. Cette écriture est appelée la décomposition sur la base factorielle.
   (a) Résultats préparatoires :
      i. Montrer que pour $N \in \mathbb{N}^\star$ donné, $\{n \in \mathbb{N} \mid n! \leqslant N\}$ est non vide et majoré.
      ii. En déduire qu'il existe un unique entier n tel que $n! \leqslant N < (n+1)!$.
      iii. On suppose que $\displaystyle\sum_{k=1}^{n} a_k k! = \sum_{k=1}^{p} b_k k!$ (les nombres a_k et b_k vérifiant les hypothèses $(\star)$). Montrer à l'aide des questions précédentes que $n = p$ puis que $a_n = b_n$.
   (b) À l'aide d'un raisonnement par récurrence forte, prouver alors que la décomposition sur la base factorielle est unique (si elle existe).
   (c) Montrer l'existence en vous aidant des résultats de la question (a).

Exercice 2.5.24 Soient A et B deux parties non vides et majorées de $\mathbb{R}$.

1. On suppose $A \subset B$. Que peut-on en déduire pour $\sup A$ et $\sup B$?
2. La partie $A \cup B$ est-elle majorée ? Si oui, que peut-on dire de sa borne supérieure ?

Exercice 2.5.25 Soient A et B deux parties non vides de $\mathbb{R}$ telles que :

$$\forall (a,b) \in A \times B \ , \ a \leqslant b$$

Montrer que $\sup A$ et $\inf B$ existent et que $\sup A \leqslant \inf B$. A-t-on nécessairement égalité ?

Exercice 2.5.26 Soient $n \in \mathbb{N}^\star$, $x_1, \cdots, x_n \in \mathbb{R}$ tels que : $\displaystyle\sum_{k=1}^{n} x_k = \sum_{k=1}^{n} x_k^2 = n$.
Montrer que $\forall k \in [\![1, n]\!]$, $x_k = 1$.

Exercice 2.5.27

1. Montrer que pour tout $(x,y) \in \mathbb{R}^2$, $E(x) + E(y) \leqslant E(x+y) \leqslant E(x) + E(y) + 1$. Pour chaque inégalité, donner un exemple d'égalité.
2. En déduire que pour tout entier $n \geqslant 1$, $nE(x) \leqslant E(nx) \leqslant nE(x) + n - 1$.
3. Montrer que pour tout $(x,y) \in \mathbb{R}^2$, $E(x) + E(y) + E(x+y) \leqslant E(2x) + E(2y)$.

Exercice 2.5.28 Montrer que pour tout entier $n \geqslant 1$ et tout $x \in \mathbb{R}$, $E\left(\dfrac{E(nx)}{n}\right) = E(x)$.

Exercice 2.5.29 Soient $n \in \mathbb{N}^\star$ et $x \in \mathbb{R}$. Démontrer que : $\displaystyle\sum_{k=0}^{n-1} E\left(x + \frac{k}{n}\right) = E(nx)$.

Exercice 2.5.30 Démontrer que pour tout $n \in \mathbb{N}$, $E\left(\dfrac{n + 2 - E\left(\frac{n}{25}\right)}{3}\right) = E\left(\dfrac{8n+24}{25}\right)$.
Indication : on pourra écrire la division euclidienne de n par 25 puis poser $k = E\left(\dfrac{r+2}{3}\right)$ et écrire la division euclidienne de $r+2$ par 3.

Exercice 2.5.31 Montrer que : $\forall n \in \mathbb{N}^\star$, $\frac{1}{\sqrt{n+1}} < 2(\sqrt{n+1} - \sqrt{n}) < \frac{1}{\sqrt{n}}$ et en déduire la partie entière de $\sum_{k=1}^{10000} \frac{1}{\sqrt{k}}$.

Exercice 2.5.32 Soient X et Y deux ensembles non vides et $f : X \times Y \longrightarrow \mathbb{R}$ une application majorée. Montrer que :

$$\sup_{(x,y) \in X \times Y} f(x,y) = \sup_{x \in X} \left(\sup_{y \in Y} f(x,y) \right) = \sup_{y \in Y} \left(\sup_{x \in X} f(x,y) \right)$$

Exercice 2.5.33 Soient $n \in \mathbb{N}^\star$, $x_1, \cdots, x_n \in \mathbb{R}^{+\star}$. On veut montrer que :

$$(x_1 + \cdots + x_n)\left(\frac{1}{x_1} + \cdots + \frac{1}{x_n}\right) \geqslant n^2$$

1. Établir le résultat en développant le produit et en regroupant les termes astucieusement.
2. On va prouver le résultat en appliquant l'inégalité de Cauchy-Schwarz. Soient $(x_1, \cdots, x_n)$ et $(y_1, \cdots, y_n)$ dans $\mathbb{R}^n$. On pose pour tout réel t,

$$P(t) = \sum_{k=1}^{n} (x_k + t y_k)^2$$

   (a) On suppose $(y_1, \cdots, y_n) \neq (0, \cdots, 0)$.

      i. Montrer que P est un polynôme du second degré.

      ii. Que peut-on dire du signe de P sur $\mathbb{R}$?

      iii. En déduire que : $\left|\sum_{k=1}^{n} x_k y_k\right| \leqslant \sqrt{\sum_{k=1}^{n} x_k^2} \times \sqrt{\sum_{k=1}^{n} y_k^2}$.

      iv. Préciser dans quel(s) cas l'inégalité est une inégalité.

      v. Retrouver le résultat de la question 1.

   (b) Montrer que l'inégalité de la question (*iii*) est encore vraie (et qu'il s'agit même d'une égalité) si $(y_1, \cdots, y_n) = (0, \cdots, 0)$.

Exercice 2.5.34 Pour tout réel x, on pose $f(x) = x - E(x)$ et on considère l'ensemble :

$$F_x = \{f(nx) \ , \ n \in \mathbb{N}^\star\}$$

1. *Quelques propriétés de la fonction f.*
   (a) Montrer que $\forall x \in \mathbb{R}$, $0 \leqslant f(x) < 1$.
   (b) Montrer que f est périodique et déterminer l'ensemble de toutes les périodes de f.
   (c) Montrer que $\forall x \in \mathbb{R}$, $\forall p \in \mathbb{N}^\star$, $f(px) = f(pf(x))$.

2. *Condition nécessaire et suffisante pour que F_x soit un ensemble fini.*
   (a) Soit $x \in \mathbb{R}$. Démontrer l'équivalence suivante :

$$x \in \mathbb{Q} \iff \exists q \in \mathbb{N}^\star \ , \ f(qx) = 0$$

(b) Soit $x = \dfrac{p}{q}$ un nombre rationnel avec $p \in \mathbb{Z}$ et $q \in \mathbb{N}^\star$.

Montrer que $f(nx) = f(rx)$ où r est le reste de la division euclidienne de n par q. Conclure que F_x est fini.

(c) La réciproque est-elle vraie ? Justifier la réponse.

3. *Dans toute la suite, on fixe un nombre réel x irrationnel.*

(a) L'ensemble F_x est-il fini ?

(b) Montrer que F_x admet une borne inférieure que l'on notera a.

(c) On suppose dans cette question que $a > 0$. On appelle p le plus petit entier tel que $pa \geqslant 1$.

i. Justifier l'existence de p et vérifier qu'il vérifie $a < \dfrac{a+1}{p}$.

ii. Montrer qu'il existe $n \in \mathbb{N}^\star$ tel que $a \leqslant f(nx) < \dfrac{a+1}{p}$.

iii. En déduire que $E(pf(nx)) = 1$ et que $f(pf(nx)) < a$.

iv. Que peut-on déduire de ce qui précède ?

(d) Montrer que : $\forall \varepsilon > 0$, $\exists n \in \mathbb{N}^\star$, $0 < f(nx) < \varepsilon$.

(e) En déduire que F_x est dense dans $[0, 1]$.

2.6 Annexe

2.6.1 Construction de $\mathbb{Z}$

La construction de l'ensemble $\mathbb{Z}$ est très intéressante et repose sur le passage au quotient (dont on a parlé lors des relations d'équivalences). C'est une démarche qui peut être adaptée à de nombreuses situations. Tout ce paragraphe est un complément qui n'est pas du tout exigible des étudiants mais qui peut assouvir la curiosité de certains.

L'idée est la suivante : un entier relatif z va être donné par un couple $(a,b) \in \mathbb{N}^2$ avec $z = b-a$. Mais on voit que ce couple n'est pas unique : on peut aussi choisir $(a+1, b+1)$. On va donc « regrouper les couples » tels que « $a-b$ » est constant, c'est-à-dire identifier deux couples (a,b) et (c,d) tels que $b-a = d-c$. Mais l'opération $-$ n'étant pas définie dans $\mathbb{N}$, on va simplement constater que cette condition équivaut à $a+d = b+c$.
De façon plus formelle, on considère l'ensemble $E = \mathbb{N} \times \mathbb{N}$ et on définit alors la relation binaire $\sim$ sur E par :

$$\forall ((a,b),(c,d)) \in E^2 \ , \ (a,b) \sim (c,d) \iff a+d = b+c$$

Proposition 2.6.1.1 *La relation $\sim$ est une relation d'équivalence sur E.*

Preuve :

Montrons que $\sim$ est une relation réflexive, symétrique et transitive.

• Réflexivité
Soit $(a,b) \in E$. Alors $a+b = b+a$ (puisque l'addition dans $\mathbb{N}$ est commutative). Par suite, $(a,b) \sim (a,b)$. Ainsi, $\sim$ est réflexive.

• Symétrie
Soient $(a,b) \in E$ et $(c,d) \in E$ tels que $(a,b) \sim (c,d)$. Alors, par définition, $a+d = b+c$, que l'on peut aussi écrire sous la forme : $c+b = d+a$ (mêmes raisons qu'avant). Par suite, $(c,d) \sim (a,b)$ prouvant ainsi que $\sim$ est symétrique.

• Transitivité.
Soient $(a,b),(c,d)$ et (e,f) trois éléments de E tels que $(a,b) \sim (c,d)$ et $(c,d) \sim (e,f)$. Par définition de la relation $\sim$, on a donc :

$$\begin{cases} a+d = b+c \\ c+f = e+d \end{cases}$$

On a alors : $a+f+d = a+d+f = b+c+f = b+e+d$, et d'après les propriétés de $\mathbb{N}$, $a+f = b+e$, c'est-à-dire $(a,b) \sim (e,f)$, ce qui prouve que $\sim$ est transitive. ⊠

Définition 2.6.1.2 Pour $x \in E$, on définit la classe d'équivalence de x par :

$$\overline{x} := \mathrm{cl}(x) = \{y \in E \ / \ y \sim x\}$$

On pose alors :

$$\mathbb{Z} = \{\overline{x} \ , \ x \in E\}$$

Sur cet ensemble $\mathbb{Z}$, on définit deux lois de composition interne de la façon suivante : pour $x \in \mathbb{Z}$ et $y \in \mathbb{Z}$, en notant $x = \overline{(a,b)}$ et $y = \overline{(c,d)}$ avec $(a,b),(c,d) \in E$,

- $x \oplus y = \overline{(a+c, b+d)}$;
- $x \otimes y = \overline{(a \times d + b \times c, a \times c + b \times d)}$.

On définit par ailleurs une relation binaire $\mathcal{R}$ définie de la façon suivante : pour $x \in \mathbb{Z}$ et $y \in \mathbb{Z}$, en notant $x = \overline{(a,b)}$ et $y = \overline{(c,d)}$ avec $(a,b),(c,d) \in E$,

$$x \mathcal{R} y \iff b + c \leqslant a + d$$

Dans ces définitions, on voit qu'il y a un problème dans le sens où le choix de $(a,b) \in E$ tel que $x = \overline{(a,b)}$ n'est pas unique, et de même pour y. On va donc commencer par démontrer que ces opérations sont bien définies.

Proposition 2.6.1.3 *Les opérations $\oplus$ et $\otimes$ sont bien définies et sont des lois de composition interne sur $\mathbb{Z}$.*

Preuve :

Soient $(a,b) \in E$, $(a',b') \in E$, $(c,d) \in E$ et $(c',d') \in E$ tels que :

$$(a,b) \sim (a',b') \ \text{ et } \ (c,d) \sim (c',d')$$

On a donc $x = \overline{(a,b)} = \overline{(a',b')}$ et $y = \overline{(c,d)} = \overline{(c',d')}$. Pour montrer que $\oplus$ et $\otimes$ sont bien définies, on doit donc démontrer que :

$$\overline{(a+c, b+d)} = \overline{(a'+c', b'+d')}$$

et

$$\overline{(ad+bc, ac+bd)} = \overline{(a'd'+b'c', a'c'+b'd')}$$

Or, par définition de la relation $\sim$, $a + b' = a' + b$ et $c + d' = c' + d$. Il s'ensuit que :

$$\begin{aligned}(b'+d')+(a+c) &= (b'+a)+(c+d')\\ &= (a'+b)+(c'+d)\\ &= (a'+c')+(b+d)\end{aligned}$$

Ces calculs sont corrects car on sait que $+$ dans $\mathbb{N}$ est associative et commutative. Ainsi :

$$(a+c,b+d)\sim(a'+c',b'+d')$$

c'est-à-dire $\overline{(a+c,b+d)}=\overline{(a'+c',b'+d')}$, ce qui montre donc que $\oplus$ est une application bien définie de $\mathbb{Z}^2$ dans $\mathbb{Z}$.

De la même façon, en notant (1) : $a+b'=a'+b$ et (2) : $c+d'=c'+d$, on a en multipliant l'égalité (1) par c' d'une part, et d'autre part, par d' :

$$\begin{aligned}a'c'+bc' &= ac'+b'c'\\ ad'+b'd' &= a'd'+bd'\end{aligned}$$

En ajoutant ces deux égalités, on obtient donc (par associativité et commutativité de $+$ et $\times$ dans $\mathbb{N}$) :

$$(3):\ a'c'+b'd'+bc'+ad'=a'd'+b'c'+ac'+bd'$$

En multipliant maintenant (2) par a d'une part, et b d'autre part, on a :

$$\begin{aligned}(1a):\ ac'+ad &= ac+ad'\\ (1b):\ bc+bd' &= bc'+bd\end{aligned}$$

En additionnant ces deux égalités, on obtient :

$$(4)\ ac'+bd'+ad+bc=ad'+bc'+ac+bd$$

Finalement, en posant $n=bc'+ad'+ac'+bd'$, on a $n\in\mathbb{N}$ et en ajoutant (3) et (4), on obtient :

$$a'c'+b'd'+ad+bc+n=a'd'+b'c'+ac+bd+n$$

Mais alors, d'après les propriétés de régularité de $+$ dans $\mathbb{N}$ (propriété 5 dans les règles admises dans $\mathbb{N}$ (voir théorème 2.2.1.1)) :

$$a'c'+b'd'+ad+bc=a'd'+b'c'+ac+bd$$

c'est-à-dire $(ad+bc,ac+bd)\sim(a'd'+b'c',a'c'+b'd')$, soit encore :

$$\overline{(ad+bc,ac+bd)}=\overline{(a'd'+b'c',a'c'+b'd')}$$

Ce qui prouve que $\otimes$ est bien définie. ⊠

Remarque : *en réalité, il aurait été plus simple de définir $\overline{\times}$ de E^2 dans E par $(a,b)\overline{\times}(c,d) = \overline{(ad+bc, ac+bd)}$ puis de montrer que cette application est constante sur les classes d'équivalences, c'est-à-dire que si $(a,b) \sim (a',b')$ et $(c,d) \sim (c',d')$, alors $(a,b)\overline{\times}(c,d) \sim (a',b')\overline{\times}(c',d')$. Ceci est plus simple car d'une part $\overline{\times}$ est commutative et d'autre part, $\sim$ est transitive. Il suffit donc de prouver que $(a,b)\overline{\times}(c,d) \sim (a',b')\overline{\times}(c,d)$.*

Proposition 2.6.1.4 *$\mathcal{R}$ est bien définie et c'est une relation d'ordre total sur $\mathbb{Z}$.*

Preuve :

• Montrons que $\mathcal{R}$ est bien définie, c'est-à-dire que si $(a,b),(a',b'),(c,d)$ et (c',d') sont quatre éléments de $E = \mathbb{N}^2$ tels que $(a,b) \sim (a',b')$ et $(c,d) \sim (c',d')$, alors :

$$\overline{(a,b)}\mathcal{R}\overline{(c,d)} \iff \overline{(a',b')}\mathcal{R}\overline{(c',d')}$$

En fait, par symétrie des rôles de (a,b), (c,d) et $(a',b'),(c',d')$, il suffit de prouver l'implication directe. Supposons donc que $\overline{(a,b)}\mathcal{R}\overline{(c,d)}$. Alors, par définition :

$$b+c \leqslant a+d$$

Or, $a+b' = a'+b$ et $c+d' = c'+d$. En ajoutant ces deux égalités, on obtient :

$$b'+a+c'+d = a'+b+c+d' \quad \text{soit encore} \quad (b'+c')+(a+d) = (a'+d')+b+c$$

Alors, en ajoutant $b'+c'$ à l'inégalité $b+c \leqslant a+d$ (licite car dans $\mathbb{N}$, on sait que $+$ est compatible avec $\leqslant$), on obtient :

$$(b'+c')+b+c \leqslant b'+c'+a+d = (a'+d')+b+c$$

D'après les propriétés de $\mathbb{N}$, on a alors : $b'+c' \leqslant a'+d'$.

• Ensuite, il est clair que $\mathcal{R}$ est réflexive car pour tout $(a,b) \in \mathbb{N}^2$, $a+b \leqslant b+a$ (la relation $\leqslant$ est réflexive dans $\mathbb{N}$).

• Montrons que $\mathcal{R}$ est antisymétrique.

Soient $(a,b),(c,d) \in \mathbb{N}^2$ tels que $\overline{(a,b)}\mathcal{R}\overline{(c,d)}$ et $\overline{(c,d)}\mathcal{R}\overline{(a,b)}$.
Alors $b+c \leqslant a+d$ et $a+d \leqslant b+c$, Or, $\leqslant$ est une relation d'ordre dans $\mathbb{N}$: en particulier, elle est antisymétrique. Par suite, $b+c = a+d$, c'est-à-dire $\overline{(a,b)} = \overline{(c,d)}$.

Ce qui prouve que $\mathcal{R}$ est antisymétrique.

• Enfin, soient $(a,b),(c,d)$ et (e,f) trois éléments de E tels que :

$$\overline{(a,b)}\mathcal{R}\overline{(c,d)} \quad \text{et} \quad \overline{(c,d)}\mathcal{R}\overline{(e,f)}$$

Par définition, $b+c \leqslant a+d$ et $d+e \leqslant f+c$. En ajoutant ces inégalités (licite car $\leqslant$ dans $\mathbb{N}$ est compatible avec l'addition), on obtient :

$$(b+c)+(d+e) \leqslant (a+d)+(f+c) \text{ soit encore } (b+e)+(c+d) \leqslant (a+f)+(c+d)$$

Par suite, $b+e \leqslant a+f$ (propriété de $\leqslant$ dans $\mathbb{N}$), c'est-à-dire $\overline{(a,b)}\mathcal{R}\overline{(e,f)}$. Ce qui prouve que $\mathcal{R}$ est transitive.
On a donc démontré que $\mathcal{R}$ est une relation d'ordre sur $\mathbb{Z}$.

• Enfin, soient $x \in \mathbb{Z}$ et $y \in \mathbb{Z}$. Soient $(a,b) \in E$ et $(c,d) \in E$ tels que $x = \overline{(a,b)}$ et $y = \overline{(c,d)}$. Puisque $\leqslant$ est une relation d'ordre total dans $\mathbb{N}$, $b+c \leqslant a+d$ ou bien $a+d \leqslant b+c$, c'est-à-dire :

$$\overline{(a,b)}\mathcal{R}\overline{(c,d)} \quad \text{ou bien} \quad \overline{(c,d)}\mathcal{R}\overline{(a,b)}$$

c'est-à-dire $x\mathcal{R}y$ ou $y\mathcal{R}x$.

⊠

Théorème 2.6.1.5 $(\mathbb{Z},\oplus,\otimes)$ *est un anneau commutatif. De plus, l'application :*

$$\begin{array}{rccc} \varphi : & \mathbb{N} & \longrightarrow & \mathbb{Z} \\ & n & \longmapsto & \overline{(0,n)} \end{array}$$

est injective et vérifie :

1. $\forall (n,m) \in \mathbb{N}^2$, $\varphi(n+m) = \varphi(n) \oplus \varphi(m)$ *et* $\varphi(n \times m) = \varphi(n) \otimes \varphi(m)$ *;*
2. $\varphi(0_{\mathbb{N}}) = 0_{\mathbb{Z}}$ *et* $\varphi(1_{\mathbb{N}}) = 1_{\mathbb{Z}}$ *;*
3. $\forall (n,m) \in \mathbb{N}^2$, $(n \leqslant m \iff \varphi(n)\mathcal{R}\varphi(m))$ *;*
4. $\varphi(\mathbb{N}) = \{z \in \mathbb{Z} \ / \ 0_{\mathbb{Z}}\mathcal{R}z\}$ *et* $\mathbb{Z} = \varphi(\mathbb{N}) \sqcup \{\ominus\varphi(n) \ , \ n \in \mathbb{N}^*\}$ *;*
5. *la relation* $\mathcal{R}$ *est compatible avec l'addition.*

Autrement dit, en identifiant $\mathbb{N}$ *et* $\varphi(\mathbb{N})$ *:*

- *l'ensemble* $\mathbb{Z}$ *contient* $\mathbb{N}$ *;*
- $\oplus_{|\mathbb{N}\times\mathbb{N}} = +$ *et* $\otimes_{|\mathbb{N}\times\mathbb{N}} = \times$ *: les opérations* $\oplus$ *et* $\otimes$ *prolongent les opérations* $+$ *et* $\times$ *dans* $\mathbb{N}$ *à* $\mathbb{Z}$ *;*
- $\mathcal{R}_{|\mathbb{N}\times\mathbb{N}} \equiv \leqslant$ *: la relation d'ordre* $\mathcal{R}$ *sur* $\mathbb{Z}$ *prolonge la relation d'ordre* $\leqslant$ *sur* $\mathbb{N}$.

Remarque : *l'ensemble* $\mathbb{N}$ *étant défini de façon unique à bijection croissante près, on peut identifier* $\mathbb{N}$ *et* $\varphi(\mathbb{N})$ *car* φ *réalise une bijection croissante de* $\mathbb{N}$ *dans* $\varphi(\mathbb{N})$.

Preuve :

• Montrons que $(\mathbb{Z}, \oplus)$ est un groupe commutatif.

∗ On a déjà vu que $\oplus$ est une loi de composition interne sur $\mathbb{Z}$.

∗ Montrons que $\oplus$ est associative.

Soit $(x, y, z) \in \mathbb{Z}^3$. Par définition, il existe $(a, b, c, d, e, f) \in \mathbb{N}^6$ tel que $x = \overline{(a, b)}$, $y = \overline{(c, d)}$ et $z = \overline{(e, f)}$. Alors, par définition de $\oplus$,

$$\begin{aligned}
(x \oplus y) \oplus z &= \overline{(a+c, b+d)} \oplus \overline{(e, f)} \\
&= \overline{((a+c)+e, (b+d)+f)} \\
&= \overline{(a+(c+e), b+(d+f))} \quad (+ \text{ est associative dans } \mathbb{N}) \\
&= \overline{(a, b)} \oplus \overline{(c+e, d+f)} \\
&= x \oplus (y \oplus z)
\end{aligned}$$

Ce qui prouve que $\oplus$ est associative.

∗ Montrons que $\oplus$ est commutative.

Soit $(x, y) \in \mathbb{Z}^2$ et soit $(a, b, c, d) \in \mathbb{N}^4$ tel que $x = \overline{(a, b)}$ et $y = \overline{(c, d)}$. Alors :

$$\begin{aligned}
x \oplus y &= \overline{(a+c, b+d)} \\
&= \overline{(c+a, d+b)} \quad (+ \text{ est commutative dans } \mathbb{N}) \\
&= \overline{(c, d)} \oplus \overline{(a, b)} \\
&= y \oplus x
\end{aligned}$$

Ce qui montre que $\oplus$ est commutative.

∗ Montrons que $0_{\mathbb{Z}} = \overline{(0_{\mathbb{N}}, 0_{\mathbb{N}})} \in \mathbb{Z}$ est l'élément neutre pour $\oplus$.

Soient $x \in \mathbb{Z}$ et $(a, b) \in \mathbb{N}^2$ tel que $x = \overline{(a, b)}$.

$$\begin{aligned}
x \oplus 0_{\mathbb{Z}} &= \overline{(a + 0_{\mathbb{N}}, b + 0_{\mathbb{N}})} \\
&= \overline{(a, b)} \quad (\text{car } 0_{\mathbb{N}} \text{ est l'élément neutre pour } + \text{ dans } \mathbb{N}) \\
&= x
\end{aligned}$$

Or, $\oplus$ est commutative donc $0_{\mathbb{Z}} \oplus x = x \oplus 0_{\mathbb{Z}} = x$ et $0_{\mathbb{Z}}$ est bien neutre pour $\oplus$.

∗ Enfin, montrons que tout élément de $\mathbb{Z}$ admet un opposé pour $\oplus$. Soient $x \in \mathbb{Z}$ et $(a,b) \in \mathbb{N}^2$ tel que $x = \overline{(a,b)}$. Posons [1] $y = \overline{(b,a)}$. Alors $y \in \mathbb{Z}$ et :

$$x \oplus y = \overline{(a+b, b+a)} = \overline{(a+b, a+b)} = \overline{(0,0)} = 0_{\mathbb{Z}}$$

En effet, $(a+b, a+b) \sim (0,0)$ donc $\overline{(a,b)} = \overline{(0,0)}$. Puisque $\oplus$ est commutative, on conclut que y est bien l'opposé de x pour $\oplus$ dans $\mathbb{Z}$.

Ainsi, on a montré que $(\mathbb{Z}, \oplus)$ est un groupe abélien.

• On a déjà prouvé que $\otimes$ est une loi de composition interne sur $\mathbb{Z}$. Montrons alors que $\otimes$ est associative, distributive par rapport à $\oplus$, admet un neutre et est commutative.
Pour simplifier la rédaction, on fixe ici $(x,y,z) \in \mathbb{Z}^3$ ainsi que $(a,b,c,d,e,f) \in \mathbb{N}^6$ tel que $x = \overline{(a,b)}$, $y = \overline{(c,d)}$ et $z = \overline{(e,f)}$ et la multiplication $\times$ dans $\mathbb{N}$ sera omise (c'est-à-dire qu'on notera ab au lieu de $a \times b$). Enfin, on ne rappellera pas les propriétés de $+$ et $\times$ dans $\mathbb{N}$.

∗ Par définition,

$$\begin{aligned}
(x \otimes y) \otimes z &= \overline{(ad+bc, ac+bd)} \otimes \overline{(e,f)} \\
&= \overline{((ad+bc)e + (ac+bd)f, (ad+bc)f + (ac+bd)e)} \\
&= \overline{(a(cf+de) + b(ce+df), a(ce+df) + b(de+cf))} \\
&= \overline{(a,b)} \times \overline{(ce+df, cf+de)} \\
&= x \otimes (y \otimes z)
\end{aligned}$$

∗ De façon similaire,

$$y \otimes x = \overline{(da+cb, ca+db)} = \overline{(ad+bc, ac+bd)} = x \otimes y$$

∗ De même,

$$\begin{aligned}
x \otimes (y \oplus z) &= \overline{(a,b)} \otimes \overline{(c+e, d+f)} \\
&= \overline{(a(d+f) + b(c+e), a(c+e) + b(d+f))} \\
&= \overline{((ad+bc) + (af+be), (ac+bd) + (ae+bf))} \\
&= \overline{(ad+bc, ac+bd)} \oplus \overline{(af+be, ae+bf)} \\
&= (x \otimes y) \oplus (x \otimes z)
\end{aligned}$$

$\otimes$ étant commutative et distributive à droite par rapport à $\oplus$, elle est aussi distributive à gauche par rapport à $\oplus$.

1. On rappelle que dans la construction on avait dit qu'un élément (a,b) correspond à l'entier $b-a$ donc son opposé est $a-b$, qui correspond à (b,a).

$*$ Enfin, en posant $1_{\mathbb{Z}} = \overline{(0_{\mathbb{N}}, 1_{\mathbb{N}})}$, on vérifie que :

$$1_{\mathbb{Z}} \otimes x = x \otimes 1_{\mathbb{Z}} = \overline{(a,b)} = x$$

Ce qui prouve que $(\mathbb{Z}, \oplus, \otimes)$ est un anneau commutatif.

• Montrons que φ est injective.

Soient $n \in \mathbb{N}$ et $p \in \mathbb{N}$ tels que $\varphi(n) = \varphi(p)$. Alors $\overline{(0,n)} = \overline{(0,p)}$, c'est-à-dire $(0,n) \sim (0,p)$ et donc $0_{\mathbb{N}} + p = n + 0_{\mathbb{N}}$, soit encore $n = p$. Ce qui prouve que φ est injective.

• Montrons la propriété 1.

Soit $(n,m) \in \mathbb{N}^2$. Alors par définition de $\oplus$ et $\otimes$,

$$\varphi(n) \oplus \varphi(m) = \overline{(0,n)} \oplus \overline{(0,m)} = \overline{(0, n+m)} = \varphi(n+m)$$

et

$$\begin{aligned} \varphi(n) \otimes \varphi(m) &= \overline{(0,n)} \otimes \overline{(0,m)} \\ &= \overline{(0 \times m + n \times 0, 0 \times 0 + n \times m)} \\ &= \overline{(0, n \times m)} \\ &= \varphi(n \times m) \end{aligned}$$

• La propriété 2 est évidente car $0_{\mathbb{Z}} = \overline{(0_{\mathbb{N}}, 0_{\mathbb{N}})}$ et $1_{\mathbb{Z}} = \overline{(0_{\mathbb{N}}, 1_{\mathbb{N}})}$.

• La propriété 3 est également triviale car pour tout $(n,m) \in \mathbb{N}^2$:

$$\varphi(n) \mathcal{R} \varphi(m) \iff \overline{(0,n)} \mathcal{R} \overline{(0,m)} \iff n + 0 \leqslant m + 0 \iff n \leqslant m$$

• Montrons à présent que $\varphi(\mathbb{N}) = \{x \in \mathbb{Z} \ / \ 0_{\mathbb{Z}} \leqslant x\}$.

Par définition de la relation $\mathcal{R}$, pour tout entier $n \in \mathbb{N}$, $\overline{(0,0)} \mathcal{R} \overline{(0,n)}$, c'est-à-dire $0_{\mathbb{Z}} \mathcal{R} \varphi(n)$. Par suite $\varphi(\mathbb{N}) \subset \{x \in \mathbb{Z} \ / \ 0_{\mathbb{Z}} \leqslant x\}$.

Réciproquement, soit $z \in \{x \in \mathbb{Z} \ / \ 0_{\mathbb{Z}} \leqslant x\}$. Il existe $(a,b) \in \mathbb{N}^2$ tel que $z = \overline{(a,b)}$ et par définition de la relation $\mathcal{R}$, $a \leqslant b$ (dans $\mathbb{N}$). D'après les propriétés de $\mathbb{N}$, il existe $n \in \mathbb{N}$ tel que $b = a+n$, c'est-à-dire $(a,b) \sim (0,n)$ et donc :

$$\overline{(a,b)} = \overline{(0,n)}$$

Ce qui prouve que $z = \overline{(0,n)} \in \varphi(\mathbb{N})$.

• Montrons que $\mathbb{Z} = \varphi(\mathbb{N}) \sqcup \ominus \varphi(\mathbb{N}^\star)$.

Puisque $\mathcal{R}$ est une relation d'ordre total, il faut et il suffit de montrer que : $\{z \in \mathbb{Z} \ / \ z \mathcal{R} 0_{\mathbb{Z}} \text{ et } z \neq 0_{\mathbb{Z}}\} = \ominus \varphi(\mathbb{N}^\star)$.

Par définition, si $n \in \mathbb{N}^\star$, $\ominus\varphi(n) = \ominus\overline{(0,n)} = \overline{(n,0)}$. Or, il est clair que $\overline{(n,0)}\mathcal{R}0_\mathbb{Z}$ et $\overline{(n,0)} \neq 0_\mathbb{Z}$ car $n \in \mathbb{N}^\star$. Par suite, on a l'inclusion :

$$\ominus\varphi(\mathbb{N}^\star) \subset \{z \in \mathbb{Z} \ / \ z\mathcal{R}0_\mathbb{Z} \text{ et } z \neq 0_\mathbb{Z}\}$$

Réciproquement, si $z \in \mathbb{Z}$ vérifie $z \neq 0_\mathbb{Z}$ et $z\mathcal{R}0_\mathbb{Z}$, alors il existe $(a,b) \in \mathbb{N}^2$ tel que $z = \overline{(a,b)}$ et on doit avoir : $b \leqslant a$ (dans $\mathbb{N}$) car $z\mathcal{R}0_\mathbb{Z}$ et $a \neq b$ car $(a,b) \not\sim (0,0)$. Il s'ensuit qu'il existe $n \in \mathbb{N}^\star$ tel que $a = b + n$ et par conséquent,

$$(a,b) \sim (n,0)$$

c'est-à-dire $\overline{(a,b)} = \overline{(n,0)}$, soit encore $z = \ominus\overline{(0,n)} = \ominus\varphi(n)$. Ce qui prouve que :

$$\{z \in \mathbb{Z} \ / \ z\mathcal{R}0_\mathbb{Z} \text{ et } z \neq 0_\mathbb{Z}\} \subset \ominus\varphi(\mathbb{N}^\star)$$

• Enfin, montrons que $\mathcal{R}$ est compatible avec $\oplus$ (et avec $\otimes$ dans le sens qui sera précisé).

Soit $(x,y,z,t) \in \mathbb{Z}^4$ tel que $x\mathcal{R}y$ et $z\mathcal{R}t$. Montrons que $(x \oplus z)\mathcal{R}(y \oplus t)$. Soit $(a,b,c,d,a',b',c',d') \in \mathbb{N}^8$ tel que : $x = \overline{(a,b)}$, $y = \overline{(c,d)}$, $z = \overline{(a',b')}$ et $t = \overline{(c',d')}$. Par définition de la relation $\mathcal{R}$, on a :

$$b + c \leqslant a + d \quad \text{et} \quad b' + c' \leqslant a' + d'$$

Puisque $+$ est compatible avec $\leqslant$ dans $\mathbb{N}$, on peut ajouter ces inégalités, ce qui donne par associativité et commutativité de $+$ dans $\mathbb{N}$:

$$(b + b') + (c + c') \leqslant (a + a') + (d + d')$$

c'est-à-dire $\overline{(a + a', b + b')}\mathcal{R}\overline{(c + c', d + d')}$, soit encore :

$$\left(\overline{(a,b)} \oplus \overline{(a',c')}\right) \mathcal{R} \left(\overline{(c,d)} \oplus \overline{(c',d')}\right)$$

c'est-à-dire $(x \oplus z)\mathcal{R}(y \oplus t)$.

Par ailleurs, si $0_\mathbb{Z}\mathcal{R}x$ et $0_\mathbb{Z}\mathcal{R}y$, alors il existe $n \in \mathbb{N}$ et $p \in \mathbb{N}$ tels que :

$$x = \varphi(n) \ \text{ et } \ y = \varphi(p)$$

Alors, $x \otimes y = \varphi(n) \otimes \varphi(p) = \varphi(np) \in \varphi(\mathbb{N})$ et par conséquent, $0_\mathbb{Z}\mathcal{R}(x \otimes y)$.

Ce qui prouve que $\mathcal{R}$ est compatible avec l'addition et la multiplication.

⊠

Remarque : *parfois les notations sont lourdes car dans cette preuve, on fait attention à bien distinguer les opérations $+$ et $\times$ dans $\mathbb{N}$ et dans $\mathbb{Z}$, et de même pour la relation $\leqslant$ dans $\mathbb{N}$ et dans $\mathbb{Z}$. Par ailleurs, beaucoup de propriétés (comme la définition de $\oplus$, $\otimes$ et $\mathcal{R}$ par exemple) sont simples à comprendre quand on comprend que « $z = b - a$ ».*

2.6.2 Ensembles finis et dénombrements

2.6.2.a Définitions et théorème fondamental

Intuitivement, on devine tous ce qu'est un ensemble fini. De même, la notion de cardinal, c'est-à-dire le nombre d'éléments est également assez intuitive. Le but de ce paragraphe est de formaliser ces notions.

Définition 2.6.2.1 On dit qu'un ensemble E est fini s'il est vide, ou bien s'il existe $n \in \mathbb{N}^\star$ et une bijection φ de $[\![1, n]\!]$ dans E.

Remarque : *de façon équivalente, E est un ensemble fini s'il est vide ou bien s'il existe $n \in \mathbb{N}^\star$ et une bijection ψ de E sur $[\![1, n]\!]$. En effet, si $\varphi : [\![1, n]\!] \longrightarrow E$ est bijective, alors $\varphi^{-1} : E \longrightarrow [\![1, n]\!]$ est également bijective.*

Remarque : *intuitivement, la définition est assez simple à comprendre. En effet, il faut penser à φ comme une numérotation des termes de E.*

Exemple 2.6.2.2 L'ensemble V des voyelles $\{a, e, i, o, u, y\}$ est un ensemble fini. En effet, soit φ l'application de $[\![1, 6]\!]$ dans V définie par :

$$\varphi(1) = a \quad ; \quad \varphi(2) = e \quad ; \quad \varphi(3) = i \quad ; \quad \varphi(4) = o \quad ; \quad \varphi(5) = u \quad \text{et} \quad \varphi(6) = y$$

Il est clair, par construction, que φ est une bijection.

Remarque : *attention, φ n'est pas du tout unique ! Il y a bien entendu plusieurs façons de « numéroter » les éléments. Si on reprend l'exemple précédent, en posant :*

$$\psi(1) = y \quad ; \quad \psi(2) = u \quad ; \quad \psi(3) = o \quad ; \quad \psi(4) = i \quad ; \quad \psi(5) = e \quad et \quad \psi(6) = a$$

ψ est aussi une bijection de $[\![1, 6]\!]$ dans V et clairement $\varphi \neq \psi$. On verra un peu plus loin qu'en revanche, s'il existe, l'entier n est unique.

Exemple 2.6.2.3 On fixe $n \geqslant 2$. Alors $\mathbb{U}_n$ est un ensemble fini.

En effet, soit $\omega = e^{i\frac{2\pi}{n}}$ et soit :

$$\begin{array}{rccc} \varphi \ : & [\![1, n]\!] & \longrightarrow & \mathbb{U}_n \\ & k & \longmapsto & \omega^{k-1} \end{array}$$

On peut commencer par remarquer que φ est bien définie, c'est-à-dire que pour tout entier $k \in [\![1, n]\!]$, $\omega^{k-1} \in \mathbb{U}_n$ (propriétés des racines n-ièmes de l'unité).
Montrons à présent que φ est une bijection.

— Montrons que φ est injective.

Soient k et l deux entiers dans $[\![1,n]\!]$ tels que $\varphi(k)=\varphi(l)$. On a alors $\omega^{k-1}=\omega^{l-1}$. Or, deux nombres complexes non nuls sont égaux si et seulement si ils ont même module et mêmes arguments (à 2π près). Par suite,

$$\begin{aligned}\varphi(k)=\varphi(l) &\iff \frac{2(k-1)\pi}{n}\equiv\frac{2(l-1)\pi}{n}\ \ [2\pi]\\ &\iff k-1\equiv l-1\ \ [n]\\ &\iff k-l\equiv 0\ \ [n]\end{aligned}$$

Il s'ensuit qu'il existe un entier $q\in\mathbb{Z}$ tel que : $k=l+qn$. Mais les conditions $k,l\in[\![1,n]\!]$ impliquent que $-(n-1)\leqslant k-l\leqslant n-1$. Par suite, $q=0$ et $k=l$.
Ce qui prouve que φ est injective.

— Montrons que φ est surjective.

Soit $z\in\mathbb{U}_n$. D'après le cours sur les nombres complexes, il existe $r\in[\![0,n-1]\!]$ tel que $z=\omega^r$. Posons $k=r+1$: alors, d'une part, $k\in[\![1,n]\!]$ et d'autre part, $\varphi(k)=\omega^{k-1}=\omega^r=z$.
Ceci montre que φ est surjective.

Ce deuxième exemple montre bien que certains résultats, bien qu'évidents, nécessitent un peu (voire beaucoup) de travail pour les établir de façon rigoureuse.

Théorème 2.6.2.4 (Fondamental) *Soient $n,p\in\mathbb{N}^\star$. S'il existe une bijection de $[\![1,n]\!]$ sur $[\![1,p]\!]$, alors $n=p$.*

Preuve :

On considère la propriété $P(n)$: « pour tout entier $p\in\mathbb{N}^\star$, s'il existe une bijection de $[\![1,p]\!]$ dans $[\![1,n]\!]$ alors $p=n$ ». Montrons par récurrence que : $\forall n\in\mathbb{N}^\star$, $P(n)$.

Initialisation :

Pour $n=1$, soit $p\in\mathbb{N}^\star$ tel qu'il existe une bijection φ de $[\![1,p]\!]$ dans $[\![1,n]\!]=\{1\}$. On a alors $\varphi(1)\in\{1\}$ donc $\varphi(1)=1$. De même, $\varphi(p)=1$.
φ étant bijective, elle est en particulier injective et donc $\varphi(1)=\varphi(p)$ implique que $p=1$ et finalement, $p=n$ (puisque $n=1$).
Ce qui montre que la propriété est vraie au rang $n=1$.

Hérédité :

On suppose la propriété vraie au rang $n\geqslant 1$: montrons qu'elle est vraie au rang $n+1$.

Soit $p \in \mathbb{N}^\star$. On suppose qu'il existe une bijection $\varphi : [\![1, p]\!] \longrightarrow [\![1, n+1]\!]$. On veut montrer que $p = n + 1$. On procède en plusieurs étapes.

• Pour commencer, φ^{-1} est une bijection de $[\![1, n + 1]\!]$ dans $[\![1, p]\!]$. En particulier, φ^{-1} est injective. Par ailleurs, $n \in \mathbb{N}^\star$ donc $n + 1 \neq 1$. On en déduit donc successivement que $\varphi^{-1}(1) \neq \varphi^{-1}(n + 1)$, puis que $[\![1, p]\!]$ contient au moins deux éléments distincts et enfin, que $p \geqslant 2$.

• Ayant prouvé que $p \geqslant 2$, on a donc $p - 1 \in \mathbb{N}^\star$. On a alors deux cas :

Premier cas : $\varphi(p) = n + 1$

Dans ce cas, considérons l'application :

$$\begin{array}{rccc} \psi & : & [\![1, p-1]\!] & \longrightarrow & [\![1, n]\!] \\ & & x & \longmapsto & \varphi(x) \end{array}$$

∗ Tout d'abord, ψ est bien définie. En effet, si $x \in [\![1, p - 1]\!]$, alors $\varphi(x) \in [\![1, n + 1]\!]$ et puisque $x \neq p$, $\varphi(x) \neq \varphi(p)$, soit encore, par hypothèse, $\varphi(x) \neq n + 1$. Il s'ensuit que $\varphi(x) \in [\![1, n]\!]$.

∗ Ensuite, φ étant injective, il est clair que ψ est injective.

∗ Enfin, soit $y \in [\![1, n]\!] \subset [\![1, n + 1]\!]$. φ étant bijective, il existe (un unique) $x \in [\![1, p]\!]$ tel que $\varphi(x) = y$. Par ailleurs, $\varphi(x) \neq \varphi(p)$ car $y \neq n + 1$ et donc $x \neq p$ (puisque φ est injective).
Il s'ensuit que $x \in [\![1, p]\!]$ et $x \neq p$, c'est-à-dire $x \in [\![1, p - 1]\!]$. Finalement, on peut donc écrire que $y = \varphi(x) = \psi(x)$. Ceci montre que ψ est surjective.

Ainsi, on a montré que si $\varphi(p) = n + 1$, il existe une bijection de ψ : de $[\![1, p - 1]\!]$ dans $[\![1, n]\!]$ avec $p - 1 \geqslant 1$. Par hypothèse de récurrence, $p - 1 = n$, c'est-à-dire $p = n + 1$.

Deuxième cas : $\varphi(p) \neq n + 1$

Dans ce cas, soit $\tau : [\![1, n + 1]\!] \longrightarrow [\![1, n + 1]\!]$ définie par :

$$\forall x \in [\![1, n + 1]\!] \ , \ \tau(x) = \begin{cases} \varphi(p) & \text{si } x = n + 1 \\ n + 1 & \text{si } x = \varphi(p) \\ x & \text{sinon} \end{cases}$$

Il est clair que $\tau \circ \tau = \mathrm{Id}_{[\![1,n+1]\!]}$. Par suite, τ est bijective. Considérons $\psi = \tau \circ \varphi$. Alors ψ est une application de $[\![1, p]\!]$ dans $[\![1, n + 1]\!]$ qui est bijective (puisque c'est la composée de deux bijections) et qui vérifie $\psi(p) = \tau(\varphi(p)) = n + 1$. D'après le premier cas, on a alors $p = n + 1$.

Ce qui montre que la propriété est vraie au rang $n + 1$ et achève la récurrence.

⊠

Théorème 2.6.2.5 (Définition du cardinal) *Soit E un ensemble fini non vide. Alors il existe un unique entier n tel que E soit en bijection avec $[\![1, n]\!]$. L'entier n est appelé le cardinal de E, et noté Card(E) ou encore $|E|$.*

Preuve :

Soit E un ensemble fini non vide. On sait alors, par définition d'un ensemble fini, qu'il existe un entier n tel que E soit en bijection avec $[\![1, n]\!]$. Il reste à prouver que l'entier n est unique.

S'il existe deux bijections $\psi : [\![1, n]\!] \longrightarrow E$ et $\varphi : [\![1, p]\!] \longrightarrow E$, alors l'application $\psi^{-1} \circ \varphi$ est une bijection de $[\![1, p]\!]$ sur $[\![1, n]\!]$ (composition de bijections). Par conséquent, d'après le théorème précédent, $n = p$. Ceci prouve l'unicité de l'entier n.

⊠

Remarque : *par convention, on pose Card$(\emptyset) = 0$.*

Proposition 2.6.2.6 *Deux ensembles finis E et F ont le même cardinal si et seulement si il existe une bijection de E sur F.*

Preuve :

• Montrons $\Longrightarrow$.
Supposons que E et F aient le même cardinal et notons $n = |E| = |F|$. On a alors deux cas :

- soit $n = 0$ et dans ce cas, $E = \emptyset = F$ et l'application vide[1] $i_\emptyset : \emptyset \longrightarrow \emptyset$ est une bijection entre E et F ;
- ou alors $n \geqslant 1$ et dans ce cas, il existe deux bijections f et g de $[\![1, n]\!]$ dans E et F, respectivement. Il s'ensuit que $\varphi = g \circ f^{-1}$ est une bijection de E dans F.

• Montrons $\Longleftarrow$.
On suppose qu'il existe une bijection φ de E sur F. On distingue à nouveau deux cas :

- si $E = \emptyset$, alors $\varphi(E) = \varphi(\emptyset) = \emptyset$ et puisque φ est surjective, $F = \varphi(E) = \emptyset$. Ainsi $|E| = 0 = |F|$. De même, si $F = \emptyset$, on applique le même raisonnement avec φ^{-1} ;

1. en effet, comme toute propriété commençant par « $\forall x \in \emptyset$ » est toujours vraie, il existe une et une seule application de $\emptyset$ dans $\emptyset$ et cette application est bien injective et surjective.

∗ si $E \neq \emptyset$ et $F \neq \emptyset$, notons $n = |E|$ et $p = |F|$. Alors il existe f et g deux bijections de $[\![1, n]\!]$ dans E et de $[\![1, p]\!]$ dans F respectivement. On en déduit que l'application $g^{-1} \circ \varphi \circ f$ est une bijection de $[\![1, n]\!]$ dans $[\![1, p]\!]$. Par suite, $n = p$.

⊠

2.6.2.b Parties de $\mathbb{N}$ et parties d'un ensemble fini

Théorème 2.6.2.7 *Soient A et B deux parties finies et disjointes d'un ensemble E. Alors $A \cup B$ est un ensemble fini et :*

$$|A \cup B| = |A| + |B|$$

Preuve :

On distingue toujours deux cas.

• Premier cas : $A = \emptyset$ ou $B = \emptyset$.
Dans ce cas, quitte à échanger les noms, on peut toujours supposer que $B = \emptyset$. On a alors : $A \cup B = A \cup \emptyset = A$ donc $A \cup B$ est un ensemble fini et $|A \cup B| = |A| = |A| + |\emptyset| = |A| + |B|$.

• Deuxième cas : $A \neq \emptyset$ et $B \neq \emptyset$.
Posons alors $n = |A|$ et $p = |B|$, avec $n, p \in \mathbb{N}^\star$. Il existe deux bijections $[\![1, n]\!] \xrightarrow{f} A$ et $[\![1, p]\!] \xrightarrow{g} B$.
L'idée est alors de numéroter les premiers termes avec f et les termes suivants avec g. Pour cela, on pose :

$$\begin{array}{ccc} [\![1, n+p]\!] & \xrightarrow{\varphi} & A \cup B \\ x & \longmapsto & \begin{cases} f(x) & \text{si } 1 \leqslant x \leqslant n \\ g(x-n) & \text{si } n+1 \leqslant x \leqslant n+p \end{cases} \end{array}$$

Montrons alors que φ est bien définie et bijective.

∗ Pour commencer, il est clair que φ est bien définie puisque si $n+1 \leqslant x \leqslant n+p$, alors $x - n \in [\![1, p]\!]$ et g est définie sur $[\![1, p]\!]$.

∗ Ensuite, montrons que φ est injective. Soient $x, x' \in [\![1, n+p]\!]$ tels que $x \neq x'$. Montrons que $\varphi(x) \neq \varphi(x')$.

▷ Si $(x, x') \in [\![1, n]\!] \times [\![n+1, n+p]\!] \cup [\![n+1, n+p]\!] \times [\![1, n]\!]$, alors soit $\varphi(x) \in A$ et $\varphi(x') \in B$ ou bien $\varphi(x) \in B$ et $\varphi(x') \in A$. Dans les deux cas de figure, comme $A \cap B = \emptyset$, $\varphi(x) \neq \varphi(x')$.

▷ Si $(x, x') \in [\![1, n]\!]^2$ (respectivement $(x, x') \in \cup[\![n+1, n+p]\!]^2$), alors $\varphi(x) = f(x)$ et $\varphi(x') = f(x')$ (respectivement $\varphi(x) = g(x-n)$ et $\varphi(x') = g(x-n)$). Or, f (respectivement g) étant injective, $x \neq x'$ entraîne $f(x) \neq f(x')$ (respectivement $x \neq x'$ entraîne $x - n \neq x' - n$ et donc $g(x-n) \neq g(x'-n)$). Ainsi, $\varphi(x) \neq \varphi(x')$.

Ainsi, dans tous les cas $\varphi(x) \neq \varphi(x')$ et φ est bien injective.

∗ Montrons enfin que φ est surjective.

Soit $y \in A \cup B$. On distingue alors deux cas :

▷ si $y \in A$, alors f étant surjective, il existe $x \in [\![1, n]\!]$ tel que $y = f(x)$. Comme $x \in [\![1, n]\!]$, on a bien $y = f(x) = \varphi(x)$ et y a bien un antécédent par φ ;

▷ de même, si $y \in B$, alors g étant surjective, il existe un entier $x \in [\![1, p]\!]$ tel que $y = g(x)$. On a alors $y = g(x + n - n)$ avec $x + n \in [\![n+1, n+p]\!]$, c'est-à-dire $y = \varphi(x+n)$.

Ceci prouve que φ est bien surjective.

Ainsi, on a montré que φ est une bijection de $[\![1, n+p]\!]$ dans $A \cup B$, avec $n + p \in \mathbb{N}^\star$. Par conséquent, $A \cup B$ est un ensemble fini et :

$$|A \cup B| = n + p = |A| + |B|$$

⊠

Proposition 2.6.2.8 *Toute partie $A \subset \mathbb{N}$ majorée est finie ; plus précisément, si A est majoré par $n \in \mathbb{N}$, alors $|A| \leqslant n + 1$.*

Preuve :

Montrons la proposition par récurrence sur $n \in \mathbb{N}$.

Initialisation :

Pour $n = 0$, A est majorée par 0. Par suite, $A = \emptyset$ ou bien $A = \{0\}$ et donc $|A| = 0$ ou $|A| = 1$. Ainsi $|A| \leqslant 0 + 1$ et la propriété est vraie au rang 0.

Hérédité :

On suppose que pour toute partie B de $\mathbb{N}$, majorée par n, B est finie et $|B| \leqslant n+1$. Soit A une partie de $\mathbb{N}$ majorée par $n+1$. On distingue deux cas.

• Si $n + 1 \notin A$, alors A est majorée par n et d'après l'hypothèse de récurrence, $|A| \leqslant n + 1$ et *a fortiori* $|A| \leqslant n + 2$.

• Si $n+1 \in A$, on pose $B = A \setminus \{n+1\}$. Alors B est majorée par n. Par hypothèse de récurrence, B est finie et $|B| \leqslant n+1$. On a alors : $A = B \cup \{n+1\}$ (réunion disjointe de deux parties finies). D'après la proposition précédente, A est un ensemble fini et $|A| = |B| + 1 \leqslant n+2$.

Ce qui montre que la propriété est vraie au rang $n+1$ et achève la récurrence.

⊠

Proposition 2.6.2.9 *Si $A \subset [\![1, n]\!]$, alors A est fini et $|A| \leqslant n$.*

Preuve :

Identique à la démonstration précédente.

⊠

Corollaire 2.6.2.10 *Si F est un ensemble fini et $f : E \longrightarrow F$ est injective, alors E est fini et $|E| \leqslant |F|$.*

Preuve :

• Si $F = \emptyset$, alors, pour qu'il existe une application $f : E \longrightarrow F$, il est nécessaire que $E = \emptyset$. E est donc fini et on a : $|E| = 0 = |F|$. *A fortiori*, $|E| \leqslant |F|$.

• Si $F \neq \emptyset$, soient $n = |F| \in \mathbb{N}^\star$ et $\varphi : F \longrightarrow [\![1, n]\!]$ une bijection. Alors, $\varphi(f(E)) \subset [\![1, n]\!]$. D'après la proposition précédente, $\varphi(f(E))$ est un ensemble fini et $p = |\varphi(f(E))| \leqslant n$.
Si $p = 0$, alors $\varphi(f(E)) = \emptyset$, donc $E = \emptyset$ et le résultat est trivialement vrai. Sinon, il existe une bijection $\psi : \varphi(f(E)) \longrightarrow [\![1, p]\!]$. On définit alors :

$$\begin{array}{rcl} \bar{f} : E & \longrightarrow & f(E) \\ x & \longmapsto & f(x) \end{array} \quad \text{et} \quad \begin{array}{rcl} \bar{\varphi} : f(E) & \longrightarrow & \varphi(f(E)) \\ x & \longmapsto & \varphi(x) \end{array}$$

Par définition de l'image d'une application, $\bar{f}$ et $\bar{\varphi}$ sont surjectives. Par ailleurs, f et φ étant injectives, il en est de même pour $\bar{f}$ et $\bar{\varphi}$. Par conséquent, $\bar{f}$ et $\bar{\varphi}$ sont des bijections. On constate alors que l'application $g = \psi \circ \bar{\varphi} \circ \bar{f}$ est la composée de trois bijections : c'est donc une bijection de E dans $[\![1, p]\!]$. Par suite, E est fini et $|E| = p$. Enfin, comme $p \leqslant n = |F|$, on a bien $|E| \leqslant |F|$.

⊠

Remarque : *dans cette démonstration, il y une idée ou propriété importante à retenir. Si $f : E \longrightarrow F$ est injective, alors $\bar{f}$, obtenue en restreignant l'ensemble d'arrivée à $f(E) = \mathrm{Im}(f)$, est automatiquement bijective.*

Corollaire 2.6.2.11 *Soient E et F deux ensembles, f une application injective de E dans F. Alors pour toute partie finie A de E, $f(A)$ est finie et $|f(A)| = |A|$.*

Preuve :

D'après la remarque, $\begin{array}{rcl} \overline{f_{|A}} : A & \longrightarrow & f(A) \\ x & \longmapsto & f(x) \end{array}$ est une bijection. A étant un ensemble fini, $f(A)$ l'est aussi et $|A| = |f(A)|$.

⊠

Théorème 2.6.2.12 *Soient A et B deux parties d'un ensemble E.*

(i) Si $A \subset B$ et B est fini, alors A est fini et $|A| \leqslant |B|$. De plus, il y a égalité si et seulement si $A = B$.

(ii) Si A et B sont finis, alors $A \cup B$ et $A \cap B$ sont des ensembles finis et on a :

$$|A \cup B| = |A| + |B| - |A \cap B|$$

Preuve :

• Montrons (i).

L'application inclusion $A \xrightarrow{i} B$ est injective. D'après le corollaire précédent, A est fini et $|A| \leqslant |B|$. Traitons alors le cas d'égalité.

∗ Si $A = B$, alors $|A| = |B|$.

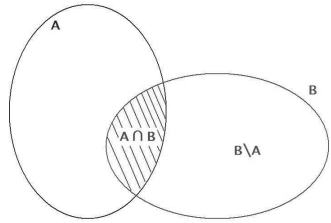
∗ Réciproquement, montrons que $|A| = |B| \Longrightarrow A = B$ par contraposée.

On suppose que $A \neq B$ et on montre que $|A| < |B|$. Par hypothèse, on a $A \subsetneq B$. Il existe donc $b \in B \setminus A$. On considère $B' = B \setminus \{b\}$. Puisque $A \subset B$ et $b \notin A$, $A \subset B'$. Par suite, $|A| \leqslant |B'|$. Enfin, B est la réunion disjointe de B' et de $\{b\}$. Par suite, $|B| = |B'| + 1$ et $|A| \leqslant |B| - 1 < |B|$.

• Montrons à présent la propriété (ii)

La démonstration a déjà été vue antérieurement (par exemple dans un cours de probabilités sur un univers fini). On rappelle ici les idées-clés.
D'une part, $A \setminus B \subset A$, donc $A \setminus B$ est un ensemble fini. De même, $B \setminus A$ et $A \cap B$ sont des ensembles finis. D'autre part, on a les réunions disjointes suivantes :

$$A \cup B = (B \setminus A) \sqcup A \quad \text{et} \quad B = (B \setminus A) \sqcup (B \cap A)$$



Par suite, $A \cup B$ et $A \cap B$ sont des ensembles finis et :

$$|A \cup B| = |B \setminus A| + |A| \quad \text{et} \quad |B| = |B \setminus A| + |A \cap B|$$

En soustrayant, on obtient le résultat.

⊠

Proposition 2.6.2.13 *Une partie $A \subset \mathbb{N}$ est finie si et seulement si elle est majorée.*

Preuve :

On a déjà prouvé la réciproque. Pour le sens direct, on procède par récurrence sur $n = |A|$.

Initialisation :

Pour $n = 0$, alors $A = \emptyset$ est majoré par tout entier.

Hérédité :

Soit A une partie de $\mathbb{N}$ telle que $|A| = n+1$. En particulier, $|A| \geqslant 1$ donc $A \neq \emptyset$: soient $a \in A$ et $B = A \setminus \{a\}$. D'après le théorème précédent, B est une partie finie de $\mathbb{N}$ et $|B| = |A| - 1 = n$.
D'après l'hypothèse de récurrence, B est majorée : soit m un majorant de B. Il est alors clair que $M = \max(a, m)$ majore A.
Ce qui montre que la propriété est vraie au rang $n + 1$ et achève la récurrence.

⊠

Proposition 2.6.2.14 *Soit A une partie non vide et finie de $\mathbb{N}$. Alors, il existe une unique bijection strictement croissante de $[\![1, n]\!]$ dans A, où $n = |A|$.*

Exercice 2.6.2.15 Prouver cette proposition.

2.6.2.c Critère de bijection pour les ensembles finis

Lemme 2.6.2.16 *Soit $f : E \longrightarrow F$ une surjection. Alors, il existe $g : F \longrightarrow E$ telle que $f \circ g = Id_F$. En particulier, g est injective.*

Preuve :

Si $F = \emptyset$, c'est clair (car alors $E = \emptyset$ et l'application vide convient). Sinon, soit $y \in F$. Alors il existe $x \in E$ tel que $y = f(x)$ (f est surjective). On choisit un tel x et on pose $g(y) = x$. Ceci définit une application g de F dans E. Par construction, pour tout $y \in F$, $y = f(x) = f(g(y))$. Ce qui prouve la première partie du lemme.
Par ailleurs, $f \circ g = \mathrm{Id}_F$ est injective, par suite g est injective.

⊠

Théorème 2.6.2.17 *Soient E et F deux ensembles finis de même cardinal $n \in \mathbb{N}$ et $f : E \longrightarrow F$ une application. Alors les propriétés suivantes sont équivalentes :*

(i) *f est injective*

(ii) *f est surjective*

(iii) *f est bijective*

Preuve :

• Montrons $(i) \Longrightarrow (ii)$.

On suppose que f est injective. Montrons que f est surjective. Puisque E est un ensemble fini et f est injective, d'après le corollaire 2.6.2.11 du paragraphe précédent, $f(E)$ est fini et $|f(E)| = |E|$. De plus, par hypothèse, $|E| = |F|$. Ainsi, on a :

$$\left.\begin{array}{l} f(E) \subset F \\ |f(E)| = |F| \end{array}\right\} \quad \text{donc, d'après le théorème 2.6.2.12, } f(E) = F.$$

Par conséquent, $f(E) = F$, c'est-à-dire que f est surjective et donc (ii).

• Montrons $(ii) \Longrightarrow (iii)$

On suppose que f est surjective. D'après le lemme, il existe $g : F \longrightarrow E$ injective telle que $f \circ g = \mathrm{Id}_F$. En appliquant le résultat $(i) \Longrightarrow (ii)$, on en déduit que g est bijective. Par suite,

$$f \circ g \circ g^{-1} = \mathrm{Id}_F \circ g^{-1} = g^{-1}$$

De plus, $g \circ g^{-1} = \mathrm{Id}_E$ et $f \circ \mathrm{Id}_E = f$. Par suite, $f = g^{-1}$ et f est bijective.

• $(iii) \Longrightarrow (i)$ est claire. ⊠

Exercice 2.6.2.18 Montrer l'implication $(ii) \Longrightarrow (iii)$ directement (c'est-à-dire sans utiliser le lemme) en considérant $\varphi : [\![1, n]\!] \longrightarrow F$ une bijection ainsi que les ensembles $E_i = f^{-1}(\{\varphi(i)\})$ (les images réciproques par f de $\{\varphi(i)\}$) pour $1 \leqslant i \leqslant n$.

Corollaire 2.6.2.19 *Soit E un ensemble fini et $f : E \longrightarrow E$. Alors :*

$$f \text{ est injective} \iff f \text{ est bijective} \iff f \text{ est surjective}$$

▶ Méthode :

Lorsqu'on veut montrer qu'une application $f : E \longrightarrow F$ est bijective, en général l'injectivité est facile à établir et c'est la surjectivité qui est plus délicate à prouver.
Lorsque E et F sont des ensembles finis, pour montrer que f est bijective, on montre souvent que :
f est injective et $|E| = |F|$.

Exercice 2.6.2.20 Soit $(A, +, \times)$ un anneau intègre. On suppose de plus que A est un ensemble fini. Montrer que A est un corps (voir aussi l'exercice 1.3.16).

Exercice 2.6.2.21 Le petit théorème de Fermat.

Soit p un nombre premier et a un entier premier avec p, c'est-à-dire que p ne divise pas a. Pour chaque entier k, on appelle q_k et r_k le quotient et le reste de la division euclidienne de ka par p. On définit alors :

$$\begin{array}{rccc} f : & [\![1, p-1]\!] & \longrightarrow & [\![1, p-1]\!] \\ & k & \longmapsto & r_k \end{array}$$

1. Montrer que f est bien définie et qu'elle est bijective.
2. Justifier alors que : $\prod_{k=1}^{p-1}(ka) \equiv \prod_{k=1}^{p-1} f(k)\,[p]$.
3. En déduire que $a^{p-1} \equiv 1\,[p]$.

Pour terminer ce paragraphe, voici quelques rappels de ce qu'on a déjà démontré ainsi que quelques conséquences.

Corollaire 2.6.2.22 *Soient E et F deux ensembles et $f : E \longrightarrow F$ une application.*

1. *Si E et F sont des ensembles finis, alors :*
   (a) *f injective $\Longrightarrow |E| \leqslant |F|$ ou de façon équivalente, $|E| > |F| \Longrightarrow f$ non injective ;*
   (b) *f surjective $\Longrightarrow |E| \geqslant |F|$ ou de façon équivalente, $|F| > |E| \Longrightarrow f$ non surjective ;*
   (c) *f bijective $\Longrightarrow |E| = |F|$.*
2. *Si F est fini et f injective, alors E est fini et $|E| \leqslant |F|$.*
3. *Si E est fini et f surjective, alors F est fini et $|F| \leqslant |E|$.*

Preuve :

On a déjà tout prouvé sauf 1(b) et 3.
Supposons que f soit surjective. D'après le lemme 2.6.2.16, il existe $g : F \longrightarrow E$ injective.

- En appliquant alors (a) à g, on en déduit 1(b) (lorsque E et F sont finis).
- Si on suppose que E est fini, alors en appliquant (2) à g, on obtient (3).

⊠

⚠ **Attention :** si E et F sont des ensembles finis mais qui ne sont pas de même cardinal et $f \in \mathcal{F}(E, F)$,

$$f \text{ injective} \not\Longleftrightarrow f \text{ bijective}$$

⚠ **Attention :** si E est un ensemble infini et $f \in \mathcal{F}(E, E)$,

$$f \text{ injective} \not\Longleftrightarrow f \text{ bijective}$$

2.6.2.d Dénombrement

2.6.2.e Cardinal d'une réunion et du complémentaire d'une partie

On a déjà démontré que si $A, B \subset E$ et si E est fini, alors $A, B, A \cap B$ et $A \cup B$ sont des ensembles finis et $|A \cup B| = |A| + |B| - |A \cap B|$.

Corollaire 2.6.2.23 *Soient E un ensemble fini et $A \subset E$. Alors $\bar{A} = E \setminus A$ est fini et $|\bar{A}| = |E| - |A|$.*

Preuve :

C'est clair car il suffit d'appliquer le théorème rappelé ci-dessus avec $B = \bar{A}$.

⊠

Corollaire 2.6.2.24 *Soient $n \in \mathbb{N}$, E un ensemble fini et $A_0, \cdots, A_n$ des parties de E, deux à deux disjointes. Alors :*

$$\left| \bigcup_{i=0}^{n} A_i \right| = \sum_{i=0}^{n} |A_i|$$

Preuve :

On démontre cette formule par récurrence sur immédiate sur n (le faire).

⊠

2.6.2.f Produit cartésien

Théorème 2.6.2.25 *Soient E et F deux ensembles finis. Alors $E \times F$ est fini et $|E \times F| = |E| \times |F|$.*

Preuve :

Pour tout $x \in E$, on pose $A_x = \{(x, y) \ , \ y \in F\}$. Les ensembles A_x, pour $x \in E$, sont tous deux à deux disjoints et leur réunion vaut $E \times F$. Par ailleurs, il est clair que pour tout $x \in E$, A_x est en bijection avec F : il est donc fini et de cardinal $|F|$.

On a alors :

$$|E \times F| = \left| \bigcup_{x \in E} A_x \right| = \sum_{x \in E} |A_x| = \sum_{x \in E} |F| = |E| \times |F|$$

⊠

Corollaire 2.6.2.26 *Si $E_1, E_2, \cdots, E_n$ sont des ensembles finis, alors $\prod_{k=1}^{n} E_k$ est un ensemble fini de cardinal $\prod_{i=1}^{n} |E_i| = |E_1| \times |E_2| \times \cdots \times |E_n|$.*

Preuve :

Une récurrence immédiate permet de conclure après avoir remarqué que :

$$\prod_{i=1}^{n+1} E_i \quad \text{est en bijection avec} \quad \left(\prod_{i=1}^{n} E_i \right) \times E_{n+1}$$

⊠

Corollaire 2.6.2.27 *Soient $n \in \mathbb{N}^\star$ et E un ensemble fini fini. Alors E^n est un ensemble fini et $|E^n| = |E|^n$.*

Preuve :

C'est une conséquence directe du corollaire précédent avec $E_i = E$ pour $1 \leqslant i \leqslant n$.

⊠

2.6.2.g Ensemble des applications de E vers F

Proposition 2.6.2.28 *Soient E et F deux ensembles finis. Alors $\mathcal{F}(E, F)$ est un ensemble fini et $|\mathcal{F}(E, F)| = |F|^{|E|}$.*

Remarque : *intuitivement c'est évident car un élément $f \in \mathcal{F}(E, F)$ est caractérisé par la donnée des images $f(x)$ pour $x \in E$. Pour chaque x dans E, il y a $|F|$ choix possibles pour $f(x)$. Il y a donc au total $|F|^{|E|}$ choix pour toutes les images.*

Preuve :

• Si $F = \emptyset$, alors $\mathcal{F}(E, F)$ est vide si $E \neq \emptyset$ et contient une seule application, qui est l'application vide si $E = \emptyset$. En convenant que $0^0 = 1$, la proposition est donc vraie lorsque $F = \emptyset$.

• On suppose à présent que $F \neq \emptyset$. De même, si $E = \emptyset$, alors $\mathcal{F}(E, F)$ contient un seul élément : l'application vide. On a donc :

$$|\mathcal{F}(E, F)| = 1 = |F|^0 = |F|^{|E|}$$

et la propriété est encore vraie.

• On se place maintenant dans le cas où E et F sont des ensembles finis non vides. Soit $n = |E|$ avec $n \geqslant 1$ et soit $\varphi : [\![1, n]\!] \longrightarrow E$ une bijection. On considère les applications suivantes :

$$\begin{array}{rccc} \psi : \mathcal{F}(E, F) & \longrightarrow & \mathcal{F}([\![1, n]\!], F) \\ f & \longmapsto & f \circ \varphi \end{array}$$

et

$$\begin{array}{rccc} \pi : \mathcal{F}([\![1, n]\!], F) & \longrightarrow & F^n \\ f & \longmapsto & (f(1), f(2), \cdots, f(n)) \end{array}$$

Il est clair que ψ et π sont bijectives (puisque φ est bijective). On a alors successivement :

- F^n est fini et π bijective, donc $\mathcal{F}([\![1, n]\!], F)$ est un ensemble fini et $|\mathcal{F}([\![1, n]\!], F)| = |F^n|$;
- $\mathcal{F}([\![1, n]\!], F)$ est fini et ψ est bijective, donc $\mathcal{F}(E, F)$ est fini et a même cardinal que $\mathcal{F}([\![1, n]\!], F)$.

Par conséquent, $\mathcal{F}(E, F)$ est bien un ensemble fini et :

$$|\mathcal{F}(E, F)| = |\mathcal{F}([\![1, n]\!], F)| = |F^n| = |F|^n = |F|^{|E|}$$

⊠

2.6.2.h Cardinal de $\mathcal{P}(E)$

Définition 2.6.2.29 Soit $A \in \mathcal{P}(E)$. On appelle fonction caractéristique de A et on note χ_A l'application :

$$\begin{array}{rccc} \chi_A : E & \longrightarrow & \{0, 1\} \\ x & \longmapsto & \begin{cases} 1 & \text{si } x \in A \\ 0 & \text{sinon} \end{cases} \end{array}$$

Proposition 2.6.2.30 *L'application* $\varphi : \mathcal{P}(E) \longrightarrow \mathcal{F}(E, \{0,1\})$ *qui à* A *associe* χ_A *est une bijection.*

Preuve :

• Montrons que φ est injective.

Soient A et B deux parties de E telles que $\varphi(A) = \varphi(B)$. Montrons que $A = B$. Soit $x \in E$. Par définition d'une fonction caractéristique, on a alors :

$$x \in A \iff \chi_A(x) = 1 \iff \varphi(A)(x) = 1$$

d'où

$$x \in A \iff \varphi(B)(x) = 1 \iff \chi_B(x) = 1 \iff x \in B$$

Ainsi, $x \in A \iff x \in B$, c'est-à-dire $A = B$ et φ est bien injective.

• Montrons que φ est surjective.

Soit $f \in \mathcal{F}(E, \{0,1\})$. Considérons :

$$A = \{x \in E \mid f(x) = 1\} = f_r^{-1}(\{1\})$$

Il est alors clair que $A \subset E$, c'est-à-dire $A \in \mathcal{P}(E)$ et par définition : $f(x) = 1 \iff x \in A$. Sachant que f ne prend que 0 et 1 comme valeurs, on a bien $f = \chi_A$. Par suite, φ est surjective.

Ainsi, φ est injective et surjective, c'est-à-dire φ est bien une bijection.

⊠

Proposition 2.6.2.31 *Soit* E *un ensemble fini. Alors* $\mathcal{P}(E)$ *est un ensemble fini et* $|\mathcal{P}(E)| = 2^{|E|}$.

Preuve :

En effet, d'après la proposition précédente, $\mathcal{P}(E)$ est en bijection avec $\mathcal{F}(E, \{0,1\})$. E étant fini, tout comme $\{0,1\}$, $\mathcal{F}(E, \{0,1\})$ est fini. Par conséquent, $\mathcal{P}(E)$ est aussi un ensemble fini et :

$$|\mathcal{P}(E)| = |\mathcal{F}(E, \{0,1\})| = 2^{|E|}$$

⊠

Remarque : *on reverra un peu plus loin une autre démonstration qui utilise les coefficients binomiaux.*

2.6.2.i Arrangements, nombres d'injections et nombres de bijections d'un ensemble dans lui-même

Proposition 2.6.2.32 *Soient E et F deux ensembles finis, $n = |F|$ et $p = |E|$. On suppose que $0 \leqslant p \leqslant n$. Alors l'ensemble $I(E,F)$ des injections de E dans F est fini (on dit aussi que c'est l'ensemble des arrangements de p éléments parmi n) et :*

$$|I(E,F)| := A_n^p = \frac{n!}{(n-p)!}$$

Remarque : *intuitivement, c'est à nouveau très simple à comprendre. En effet, si on note $x_1, \cdots, x_p$ les éléments de E et on se donne f une injection de E dans F. Alors :*

- *pour $f(x_1)$, il y a n choix possibles (les n éléments de F) ;*
- *pour $f(x_2)$, il y a $n-1$ choix possibles (les éléments de $F \setminus \{f(x_1)\}$) ;*

$$\vdots$$

- *pour $f(x_p)$, il y a $n-(p-1)$ choix possibles (les éléments de $F \setminus \{f(x_1), \cdots, f(x_{p-1})\}$).*

Au total, il y a donc $n \times (n-1) \times (n-(p-1))$ possibilités, c'est-à-dire $\dfrac{n!}{(n-p)!}$.

Preuve :

Soit $n \in \mathbb{N}$ fixé. On démontre la proposition en raisonnant par récurrence finie sur $p \in [\![0, n]\!]$.

Initialisation :

Pour $p = 0$, on a $E = \emptyset$ et $\mathcal{F}(\emptyset, F) = \{i_{\emptyset,F}\}$ (l'application vide). L'application vide est injective donc $|I(E,F)| = 1$. De même, $A_n^0 = \dfrac{n!}{n!} = 1$. La propriété est vraie au rang $p = 0$.

Hérédité :

Si $n = 0$, c'est fini. Sinon, on suppose la propriété vraie au rang $p < n$. Montrons qu'elle est vraie au rang $p+1$.
Soit E un ensemble de cardinal $p+1$, avec $p+1 \leqslant n$. Alors $E \neq \emptyset$, donc il existe $a \in E$. On fixe un tel a, on pose $E' = E \setminus \{a\}$ et on considère l'application :

$$\begin{array}{cccc} \varphi & I(E,F) & \longrightarrow & I(E',F) \\ & f & \longmapsto & f_{|E'} \end{array}$$

• D'une part, φ est bien définie. En effet, si $f : E \longrightarrow F$ est injective, alors $f_{|E'}$ est encore injective.

• D'autre part, si $g \in I(E', F)$ alors $\varphi_r^{-1}(\{g\})$ est l'ensemble des applications f injectives de E dans F telles que $f_{|E'} = g$. Il est clair que ces applications f sont les applications telles que $f(a) \notin g(E')$, c'est-à-dire que $|\varphi^{-1}(\{g\})| = n - p$. On en déduit alors que :

$$\begin{aligned} |I(E,F)| &= \left| \bigsqcup_{g \in I(E',F)} \varphi^{-1}(\{g\}) \right| \\ &= \sum_{g \in I(E',F)} |\varphi^{-1}(\{g\})| \\ &= \sum_{g \in I(E',F)} (n-p) \\ &= (n-p) \times |I(E',F)| \\ &= (n-p)\frac{n!}{(n-p)!} \\ &= \frac{n!}{(n-(p+1))!} \end{aligned}$$

Ce qui montre que la propriété est vraie au rang $p+1$ et achève la récurrence.

⊠

Remarque : *on a supposé que* $0 \leqslant p \leqslant n$. *Que dire de* $I(E,F)$ *lorsque* $|E| > |F|$ *?*

Corollaire 2.6.2.33 *Si* $|E| = n$, *alors l'ensemble des permutations de* E *(c'est-à-dire l'ensemble des bijections de* E*), noté* $\sigma(E)$ *est un ensemble fini et son cardinal est* $n!$.

Preuve :

Si E est fini de cardinal n, alors une application $f : E \longrightarrow E$ est injective si et seulement si elle est bijective. Par suite, $\sigma(E) = I(E,E)$ est fini et son cardinal est :

$$|\sigma(E)| = |I(E,E)| = \frac{n!}{(n-n)!} = n!$$

⊠

2.6.2.j Combinaisons et coefficients binomiaux

Proposition 2.6.2.34 *Soit E un ensemble fini de cardinal n. Soit $p \in \mathbb{N}$ tel que $p \leqslant n$. On note $\mathcal{P}_p(E)$ l'ensemble des parties de E ayant p éléments, c'est-à-dire*

$$\mathcal{P}_p(E) = \{A \in \mathcal{P}(E) \ / \ |A| = p\}$$

Alors $\mathcal{P}_p(E)$ est un ensemble fini et $|\mathcal{P}_p(E)| = \dfrac{n!}{p!(n-p)!} = \binom{n}{p}$.

Remarque : *pour une explication plus intuitive ainsi que plus de propriétés, vous pouvez lire un cours de probabilités sur un univers fini.*

Preuve :

• Tout d'abord, comme E est fini, d'après les résultats précédents, $\mathcal{P}(E)$ est fini, et donc $\mathcal{P}_p(E) \subset \mathcal{P}(E)$ est également un ensemble fini.

• Soit I l'ensemble des injections de $[\![1, p]\!]$ dans E et soit φ l'application :

$$\begin{array}{rccc} \varphi : & I & \longrightarrow & \mathcal{P}_p(E) \\ & f & \longmapsto & f([\![1, p]\!]) \end{array}$$

∗ Tout d'abord, φ est bien définie puisque si $f \in I$, f est injective et donc $|f([\![1, p]\!])| = |[\![1, p]\!]\ | = p$.

∗ Par ailleurs, si $A \in \mathcal{P}_p(E)$, alors :

$$\varphi_r^{-1}(\{A\}) = \{f \in \mathcal{F}([\![1, p]\!], E) \ / \ f \text{ est injective et } f([\![1, p]\!]) = A\}$$

De plus, $|A| = p$ donc une application de $[\![1, p]\!]$ dans A est injective si et seulement si elle est bijective. Il s'ensuit que $\varphi_r^{-1}(\{A\})$ est en bijection avec l'ensemble :

$$S = \{f \in \mathcal{F}([\![1, p]\!], A) \ / \ f \text{ est bijective}\}$$

Alors, d'après le paragraphe précédent, $|\varphi^{-1}(\{A\})| = |S| = p!$. Par conséquent,

$$|I| = \left| \bigsqcup_{A \in \mathcal{P}_p(E)} \varphi^{-1}(\{A\}) \right| = \sum_{A \in \mathcal{P}_p(E)} |\varphi^{-1}(\{A\})| = \sum_{A \in \mathcal{P}_p(E)} p!$$

c'est-à-dire $|I| = p! \times |\mathcal{P}_p(E)|$.

⊠

2.6.2.k Propriétés des coefficients binomiaux

Proposition 2.6.2.35 *Soient n et p deux entiers tels que $0 \leqslant p \leqslant n$. Alors :*

(i) $\binom{n}{p} = \binom{n}{n-p}$

(ii) $\sum_{p=0}^{n} \binom{n}{p} = 2^n$

(iii) Si $n \geqslant 1$ et $p \geqslant 1$, $\binom{n-1}{p-1} + \binom{n-1}{p} = \binom{n}{p}$ *(formule du triangle de Pascal)*

Preuve :

Soit E un ensemble de cardinal n.

• Montrons (i).
On sait que pour toute partie A de E, $\overline{\overline{A}} = A$ et $|\overline{A}| = n - |A|$. On en déduit donc que l'application

$$\begin{array}{rcl} \varphi : \mathcal{P}_p(E) & \longrightarrow & \mathcal{P}_{n-p}(E) \\ A & \longmapsto & \overline{A} \end{array}$$

est une bijection (sa bijection réciproque étant $\psi : \mathcal{P}_{n-p}(E) \longrightarrow \mathcal{P}_p(E)$ qui à A associe $\complement_E(A) = \overline{A}$). On en déduit que $|\mathcal{P}_p(E)| = |\mathcal{P}_{n-p}(E)|$.

• Montrons (ii).
On a $\mathcal{P}(E) = \bigsqcup_{p=0}^{n} \mathcal{P}_p(E)$. La réunion étant finie et disjointe, on a :

$$2^n = 2^{|E|} = |\mathcal{P}(E)| = \sum_{p=0}^{n} |\mathcal{P}_p(E)| = \sum_{p=0}^{n} \binom{n}{p}$$

• Montrons (iii).
On fixe un élément x de E. Alors l'ensemble des parties de E ayant p éléments est la réunion disjointe de deux sous-parties : les parties de E ayant p éléments et qui ne contiennent pas x (il y en a $\binom{n-1}{p}$) et les parties de E ayant p éléments et contenant x (il y en a $\binom{n-1}{p-1}$).

⊠

Remarque : *bien entendu, on peut aussi retrouver ces formules par le calcul brutal direct.*

Il y a bien entendu de nombreuses autres propriétés des coefficients binomiaux. Par exemple, la formule de Pascal itérée ou la relation de Van der Monde. Le lecteur intéressé pourra consulter plus de détails sur ces propriétés dans n'importe quel ouvrage de licence qui aborde par exemple les probabilités finies.

Chapitre 3

Suites de nombres réels ou complexes

Prérequis : dans tout ce chapitre, les notions suivantes sont supposées connues :

- le cours de logique (implications, équivalences, prédicat) ;
- notion d'ensemble ;
- relation d'équivalence ; relation d'ordre, borne inférieure et borne supérieure ;
- l'ensemble $\mathbb{N}$ et toutes ses propriétés ; ensemble $\mathbb{Z}$;
- l'ensemble $\mathbb{R}$ et toutes ses propriétés ;
- applications monotones ; injections, surjections et bijections ;
- structures usuelles : groupes, anneaux et corps ; morphismes de groupes ou d'anneaux ;
- nombres complexes : module, partie réelle et partie imaginaire ;
- notations o et O pour les fonctions.

Aucune connaissance spécifique sur les suites n'est supposée connue.

3.1 Suites de nombres réels

3.1.1 Généralités

Définition 3.1.1.1 On appelle suite de nombre réels toute application $u : \mathbb{N} \longrightarrow \mathbb{R}$. On pose pour tout entier n, $u(n) = u_n$ et on désigne la suite par $u = (u_n)_{n\in\mathbb{N}}$.

On dit aussi que u_n est le terme général de la suite $(u_n)_{n\in\mathbb{N}}$, ou encore, pour $n \in \mathbb{N}$ donné, que u_n est le n-ième terme de la suite $(u_n)_{n\in\mathbb{N}}$ ou le terme d'indice n.

Exemple 3.1.1.2 On définit une suite $(u_n)_{n\in\mathbb{N}}$ en posant $u_n = \cos(n)$ pour tout entier n. On peut aussi définir une suite par une relation de récurrence. Par exemple, $u_0 = 1$ et pour tout entier n, $u_{n+1} = 3u_n$ définit également une suite.

Remarques :

- *de façon équivalente, une suite réelle est une famille de nombres réels indexée par* $\mathbb{N}$ *;*
- *on peut étendre la notion de suite aux applications* $u : [\![n_0, +\infty[\![\longrightarrow \mathbb{R}$ *ou encore* $u : \mathbb{Z} \longrightarrow \mathbb{R}$*. Dans le premier cas, on parle de suite définie à partir du rang* n_0*. Dans le second cas, on parle de famille de réels indexée par* $\mathbb{Z}$*.*

Définition 3.1.1.3 Soit $(u_n)_{n\in\mathbb{N}}$ une suite réelle. On dit que $(u_n)_{n\in\mathbb{N}}$ est :

- croissante si $\forall (n,p)^2 \in \mathbb{N}^2$, $(n \leqslant p \Longrightarrow u_n \leqslant u_p)$;
- strictement croissante si $\forall (n,p)^2 \in \mathbb{N}^2$, $(n < p \Longrightarrow u_n < u_p)$;
- décroissante si $\forall (n,p)^2 \in \mathbb{N}^2$, $(n \leqslant p \Longrightarrow u_n \geqslant u_p)$;
- strictement décroissante si $\forall (n,p) \in \mathbb{N}^2$, $(n < p \Longrightarrow u_n > u_p)$;
- monotone (respectivement strictement monotone) si elle est soit croissante, soit décroissante (respectivement strictement).

Proposition 3.1.1.4 *Soit* $(u_n)_{n\in\mathbb{N}}$ *une suite de nombres réels. Alors* $(u_n)_{n\in\mathbb{N}}$ *est croissante (respectivement décroissante) si et seulement si* $\forall n \in \mathbb{N}$, $u_n \leqslant u_{n+1}$ *(respectivement :* $\forall n \in \mathbb{N}$, $u_n \geqslant u_{n+1}$*).*

Preuve :

Traitons le cas des suites croissantes. Le cas des suites décroissantes s'obtient alors en appliquant le résultat à $(-u_n)_{n\in\mathbb{N}}$.

• L'implication $\Longrightarrow$ est évidente.

• Montrons $\Longleftarrow$

On suppose que : $\forall n \in \mathbb{N}$, $u_n \leqslant u_{n+1}$. Montrons que la suite $(u_n)_{n\in\mathbb{N}}$ est croissante. Soit $n \in \mathbb{N}$. On montre par récurrence immédiate que : $\forall k \in \mathbb{N}$, $u_n \leqslant u_{n+k}$. Soit $p \in \mathbb{N}$ tel que $p \geqslant n$. En prenant $k = p - n \in \mathbb{N}$, on obtient $u_n \leqslant u_p$.

⊠

Exemple 3.1.1.5 Considérons la suite $(u_n)_{n\in\mathbb{N}}$ définie par : $\forall n \in \mathbb{N}$, $u_n = n^2$. Alors $(u_n)_{n\in\mathbb{N}}$ est une suite strictement croissante. En effet, pour tout entier n,

$$u_{n+1} - u_n = 2n + 1 > 0$$

Exemple 3.1.1.6 Considérons la suite $(u_n)_{n\in\mathbb{N}}$ définie par son premier terme $u_0 = \pi$ et la relation de récurrence : $\forall n \in \mathbb{N}$, $u_{n+1} = -u_n^2 + 3u_n - 4$. Alors :

$$\forall n \in \mathbb{N} \text{ , } u_{n+1} - u_n = -u_n^2 + 2u_n - 4 < 0$$

Par conséquent, $(u_n)_{n\in\mathbb{N}}$ est strictement décroissante.

Enfin, on va traiter un dernier exemple pour vous éviter de commettre une erreur grave et fréquente.

Exercice 3.1.1.7 On considère la suite définie par $u_0 = 1$ et $\forall n \in \mathbb{N}$, $u_{n+1} = \sin(u_n)$. (On justifiera un peu plus tard la bonne définition de cette suite.)

1. Montrer que pour tout $n \in \mathbb{N}$, $u_n \in [0, \frac{\pi}{2}]$.
2. Démontrer que pour tout réel $x \geqslant 0$, $\sin(x) \leqslant x$.
3. En déduire les variations de la suite $(u_n)_{n\in\mathbb{N}}$.
4. Quelles sont les variations de la fonction sinus sur $[0, \frac{\pi}{2}]$?
5. Conclusions ?

⚠ **Attention :** pour une suite de la forme $u_{n+1} = f(u_n)$, les variations de la suite $(u_n)_{n\in\mathbb{N}}$ ne sont pas forcément les mêmes que les variations de f !!!

Définition 3.1.1.8 Soit $(u_n)_{n\in\mathbb{N}}$ une suite réelle. On dit que $(u_n)_{n\in\mathbb{N}}$ est :

- majorée s'il existe un réel M tel que : $\forall n \in \mathbb{N}$, $u_n \leqslant M$;
- minorée s'il existe un réel m tel que : $\forall n \in \mathbb{N}$, $m \leqslant u_n$;
- bornée si elle est à la fois majorée et minorée.

Exemple 3.1.1.9 Considérons les suites suivantes :

- $\forall n \in \mathbb{N}$, $u_n = n$. Alors $(u_n)_{n\in\mathbb{N}}$ est minorée (puisque par exemple, pour tout entier n, $0 \leqslant u_n$) mais n'est pas majorée.
- Soit v la suite définie par : $\forall n \in \mathbb{N}$, $v_n = -\ln(n+1)$. $(v_n)_{n\in\mathbb{N}}$ est majorée mais n'est pas minorée.
- La suite $(w_n)_{n\in\mathbb{N}}$ de terme général $w_n = 3 + \cos(n)$ est une suite bornée puisque : $\forall n \in \mathbb{N}$, $2 \leqslant w_n \leqslant 4$.

Proposition 3.1.1.10 *Soit $(u_n)_{n\in\mathbb{N}}$ une suite réelle. Alors, la suite $(u_n)_{n\in\mathbb{N}}$ est bornée si et seulement si* $\exists M \geqslant 0$, $\forall n \in \mathbb{N}$, $|u_n| \leqslant M$.

Preuve :

• Montrons $\Longleftarrow$

S'il existe $M \geqslant 0$ tel que $\forall n \in \mathbb{N}$, $|u_n| \leqslant M$, alors pour tout entier n, $-M \leqslant u_n \leqslant M$ et la suite $(u_n)_{n\in\mathbb{N}}$ est bornée.

• Montrons $\Longrightarrow$

Si $(u_n)_{n\in\mathbb{N}}$ est bornée, alors, par définition, il existe deux réels m et M tels que : $\forall n \in \mathbb{N}$, $m \leqslant u_n \leqslant M$. Posons $K = \max\{|m|, |M|\}$. Il est clair que $K \geqslant 0$ et que :

$$\forall n \in \mathbb{N} \text{ , } |u_n| \leqslant K$$

⊠

Exercice 3.1.1.11 Soit $(u_n)_{n\in\mathbb{N}}$ la suite définie par $u_0 \in [-1, 1]$ et la relation de récurrence :

$$\forall n \in \mathbb{N} \text{ , } u_{n+1} = \frac{1}{(n+1)^2} \sum_{k=0}^{n} (k+1) u_k u_{n-k}$$

Montrer que $(u_n)_{n\in\mathbb{N}}$ est bornée.

3.1.2 Opérations sur les suites

Définition 3.1.2.1 On munit l'ensemble $\mathbb{R}^{\mathbb{N}}$ des suites réelles de trois opérations et d'une relation binaire :

- une addition, notée $+$, définie par :
$$\forall (u,v) \in \mathbb{R}^{\mathbb{N}} \times \mathbb{R}^{\mathbb{N}} \ , \ \forall n \in \mathbb{N} \ , \ (u+v)_n = u_n + v_n$$
- une multiplication interne, notée $\times$, définie par :
$$\forall (u,v) \in \mathbb{R}^{\mathbb{N}} \times \mathbb{R}^{\mathbb{N}} \ , \ \forall n \in \mathbb{N} \ , \ (uv)_n = u_n \times v_n$$
- une multiplication externe, notée $\cdot$, $\mathbb{R} \times \mathbb{R}^{\mathbb{N}} \longrightarrow \mathbb{R}^{\mathbb{N}}$ définie par :
$$\forall \lambda \in \mathbb{R} \ , \ \forall u \in \mathbb{R}^{\mathbb{N}} \ , \ \forall n \in \mathbb{N} \ , \ (\lambda \cdot u)_n = \lambda \times u_n$$
- une relation binaire, notée $\leqslant$ et définie par :
$$\forall (u,v) \in \mathbb{R}^{\mathbb{N}} \times \mathbb{R}^{\mathbb{N}} \ , \ (u \leqslant v \iff \forall n \in \mathbb{N} \ , \ u_n \leqslant v_n)$$

Proposition 3.1.2.2 *$(\mathbb{R}^{\mathbb{N}}, +, \times)$ est un anneau commutatif et $(\mathbb{R}^{\mathbb{N}}, \leqslant)$ est un ensemble partiellement ordonné.*

Proposition 3.1.2.3 *Plus généralement, si E est un ensemble quelconque, $\mathcal{F}(E, \mathbb{R})$ est un anneau commutatif et un ensemble ordonné avec les opérations et la relation suivantes :*

- *addition dans $\mathcal{F}(E, \mathbb{R})$: pour $f, g \in \mathcal{F}(E, \mathbb{R})$, on définit $f + g$ par :*
$$\begin{array}{ccc} E & \xrightarrow{f+g} & \mathbb{R} \\ x & \longmapsto & f(x) + g(x) \end{array}$$
- *multiplication interne dans $\mathcal{F}(E, \mathbb{R})$: pour $f, g \in \mathcal{F}(E, \mathbb{R})$, on définit $f \times g$ par :*
$$\begin{array}{ccc} E & \xrightarrow{fg} & \mathbb{R} \\ x & \longmapsto & f(x) \times g(x) \end{array}$$
- *comparaison dans $\mathcal{F}(E, \mathbb{R})$: pour $f, g \in \mathcal{F}(E, \mathbb{R})$, on définit $f \leqslant g$ par :*
$$\forall x \in E \ , \ f(x) \leqslant g(x)$$

Preuve :

Montrons que $(\mathcal{F}(E,\mathbb{R}),+,\times)$ est un anneau commutatif, c'est-à-dire :

1. $(\mathcal{F}(E,\mathbb{R}),+)$ est un groupe abélien ;
2. $\times$ est associative, a un élément neutre et $\times$ est commutative ;
3. $\times$ est distributive par rapport à $+$.

• Montrons (1).

∗ Montrons que la loi $+$ est associative.
Soient $f,g,h \in \mathcal{F}(E,\mathbb{R})$. Alors pour tout $x \in E$,

$$\begin{aligned}(f+(g+h))(x) &= f(x)+(g+h)(x)\\ &= f(x)+g(x)+h(x) \quad \text{(la loi + est associative)}\\ &= (f+g)(x)+h(x)\\ &= ((f+g)+h)(x)\end{aligned}$$

Ceci étant vrai pour tout $x \in E$, les applications sont égales : $f+(g+h)=(f+g)+h$ et $+$ est associative.

∗ On note $0_{\mathcal{F}(E,\mathbb{R})}$ l'application constante égale à 0 : $\begin{array}{ccc} E & \overset{0_{\mathcal{F}(E,\mathbb{R})}}{\longrightarrow} & \mathbb{R} \\ x & \longmapsto & 0 \end{array}$.
Alors $0_{\mathcal{F}(E,\mathbb{R})}$ est clairement neutre pour la loi $+$.

∗ Montrons enfin que tout élément possède un opposé.
Soit $f \in \mathcal{F}(E,\mathbb{R})$. Clairement, l'application : $\begin{array}{ccc} E & \overset{g}{\longrightarrow} & \mathbb{R} \\ x & \longmapsto & -f(x) \end{array}$
vérifie $f+g=g+f=0_{\mathcal{F}(E,\mathbb{R})}$.

∗ Enfin, il est clair que $+$ est commutative puisque l'addition dans $\mathbb{R}$ l'est.

• Montrons (2).

∗ $\times$ est associative : même preuve que pour l'addition puisque la multiplication dans $\mathbb{R}$ est, elle aussi, associative.

∗ Notons $1_{\mathcal{F}(E,\mathbb{R})}$ l'application constante égale à 1 : $\begin{array}{ccc} E & \overset{1_{\mathcal{F}(E,\mathbb{R})}}{\longrightarrow} & \mathbb{R} \\ x & \longmapsto & 1 \end{array}$.
Alors $1_{\mathcal{F}(E,\mathbb{R})}$ est clairement neutre pour la loi $\times$.

∗ $\times$ est commutative découle clairement du fait que la multiplication dans $\mathbb{R}$ est commutative.

• Montrons (3)

Ceci découle du fait que la multiplication dans $\mathbb{R}$ est distributive par rapport à l'addition dans $\mathbb{R}$. En effet, soient $f, g, h \in \mathcal{F}(E, \mathbb{R})$, alors pour tout $x \in E$, on a :

$$\begin{aligned}(f \times (g+h))(x) &= f(x) \times ((g+h)(x)) \\ &= f(x) \times (g(x) + h(x))\end{aligned}$$

d'où

$$\begin{aligned}(f \times (g+h))(x) &= f(x) \times g(x) + f(x) \times h(x) \\ &= (f \times g)(x) + (f \times h)(x) \\ &= (f \times g + f \times h)(x)\end{aligned}$$

Par suite, $f \times (g+h) = f \times g + f \times h$ et $\times$ est distributive à droite par rapport à $+$. $\times$ étant commutative, elle est aussi distributive à gauche par rapport à $+$.

• Montrons que $(\mathcal{F}(E, \mathbb{R}), \leqslant)$ est un ensemble ordonné.

∗ Tout d'abord, il est clair que $\leqslant$ est bien une relation binaire sur $\mathcal{F}(E, \mathbb{R})$.

∗ Réflexivité :

soit $f \in \mathcal{F}(E, \mathbb{R})$. Alors pour tout $x \in E$, $f(x) \leqslant f(x)$ donc $f \leqslant f$ et $\leqslant$ est réflexive.

∗ Antisymétrie :

soient $f, g \in \mathcal{F}(E, \mathbb{R})$ telles que $f \leqslant g$ et $g \leqslant f$. Alors pour tout $x \in E$, $f(x) \leqslant g(x)$ et $g(x) \leqslant f(x)$. La relation $\leqslant$ dans $\mathbb{R}$ est une relation d'ordre donc pour tout $x \in E$, $f(x) = g(x)$. Ceci est vrai pour tout x dans E, donc les applications f et g sont égales. $\leqslant$ est antisymétrique.

∗ Transitivité :

soient $f, g, h \in \mathcal{F}(E, \mathbb{R})$ telles que $f \leqslant g$ et $g \leqslant h$. Soit $x \in E$. Alors $f(x) \leqslant g(x)$ et $g(x) \leqslant h(x)$. Or, la relation $\leqslant$ sur $\mathbb{R}$ est une relation d'ordre donc transitive : par suite, $f(x) \leqslant h(x)$. Ceci étant vrai pour tout x de E, on a $f \leqslant h$ et $\leqslant$ est transitive.

Ce qui prouve que $(\mathcal{F}(E, \mathbb{R}), \leqslant)$ est un ensemble ordonné.

⊠

Remarques :

• $(\mathbb{R}^{\mathbb{N}}, +, \times)$ *n'est pas un anneau intègre (et donc n'est pas un corps) puisque :*

$$\exists u, v \in \mathbb{R}^{\mathbb{N}} \text{ , } u \neq 0_{\mathbb{R}^{\mathbb{N}}} \text{ et } v \neq 0_{\mathbb{R}^{\mathbb{N}}} \text{ et } u \times v = 0_{\mathbb{R}^{\mathbb{N}}}$$

Par exemple, si on définit les suites u et v par :

$$\begin{cases} \text{pour tout entier } n,\ u_{2n} = 0 \text{ et } u_{2n+1} = 1\ ; \\ \text{pour tout entier } n,\ v_{2n} = 1 \text{ et } v_{2n+1} = 0. \end{cases}$$

Alors, $\forall n \in \mathbb{N}$, $u_n \times v_n = 0$, c'est-à-dire $u \times v = 0$ et pourtant, ni u, ni v ne sont égales à la suite nulle.

- *$(\mathbb{R}^{\mathbb{N}}, \leqslant)$ est partiellement ordonné, c'est-à-dire que l'ordre n'est pas total. En effet, si on pose pour tout entier $n \in \mathbb{N}$, $u_n = n$ et $v_n = 1$ alors :*
  - *$u_0 < v_0$ donc $v \not\leqslant u$;*
  - *de même, $v_2 < u_2$ donc $u \not\leqslant v$.*

  Ceci prouve qu'il existe deux éléments de $\mathbb{R}^{\mathbb{N}}$ qu'on ne peut pas comparer pour la relation d'ordre $\leqslant$.

- *La relation $\leqslant$ sur $\mathcal{F}(\mathbb{N}, \mathbb{R})$ est compatible avec les lois $+$ et $\times$ (comme pour les nombres réels) :*

$$\forall u, v, w, q \in \mathbb{R}^{\mathbb{N}},\ \begin{cases} u \leqslant v \\ \text{et} \\ w \leqslant q \end{cases} \Longrightarrow u+w \leqslant v+q \text{ et } \begin{cases} 0 \leqslant u \leqslant v \\ \text{et} \\ 0 \leqslant w \leqslant q \end{cases} \Longrightarrow u \times w \leqslant v \times q$$

- *Si $u \in \mathbb{R}^{\mathbb{N}}$, on peut aussi définir la suite $|u|$ par la relation :*

$$\forall n \in \mathbb{N}\ ,\ |u|(n) = |u_n|$$

Il est alors clair que u est bornée si et seulement si $|u|$ est majorée.

Proposition 3.1.2.4 *L'ensemble $(\mathbb{R}^{\mathbb{N}}, +, \cdot)$ est un espace vectoriel, c'est-à-dire que $(\mathbb{R}^{\mathbb{N}}, +)$ est un groupe abélien et la multiplication externe vérifie pour tout $(\lambda, \mu) \in \mathbb{R}^2$ et pour tout $(u, v) \in \mathbb{R}^{\mathbb{N}} \times \mathbb{R}^{\mathbb{N}}$:*

$$(\lambda+\mu)\cdot u = \lambda\cdot u + \mu\cdot v\ ;\ \lambda\cdot(u+v) = \lambda\cdot u + \lambda\cdot v\ ;\ \lambda\cdot(\mu\cdot u) = (\lambda\times\mu)\cdot u\ ;\ 1_{\mathbb{R}}\cdot u = u$$

Preuve :

Ceci découle du fait que la multiplication dans $\mathbb{R}$ est associative, distributive par rapport à l'addition et que $1_{\mathbb{R}}$ est neutre pour la multiplication. Je vous laisse vérifier ces propriétés par vous-même. La notion d'espace vectoriel sera étudiée au chapitre 4 : il ne faut donc pas se focaliser sur le vocabulaire pour le moment.

⊠

Proposition 3.1.2.5 *On note $\mathcal{B}(\mathbb{N},\mathbb{R})$ l'ensemble des suites réelles bornées. Alors $(\mathcal{B}(\mathbb{N},\mathbb{R}),+,\times)$ est un sous-anneau de $\mathbb{R}^{\mathbb{N}}$ et est stable par combinaisons linéaires, c'est-à-dire :*

$$\forall (u,v)\in\mathcal{B}(\mathbb{N},\mathbb{R})^2\ ,\ \forall(\lambda,\mu)\in\mathbb{R}^2\ ,\ (\lambda\cdot u+\mu\cdot v)\in\mathcal{B}(\mathbb{N},\mathbb{R})$$

Preuve :

• Montrons que $\mathcal{B}(\mathbb{N},\mathbb{R})$ est un sous-anneau de $\mathbb{R}^{\mathbb{N}}$, c'est-à-dire :

(i) $1_{\mathbb{R}^{\mathbb{N}}}\in\mathcal{B}(\mathbb{N},\mathbb{R})$;

(ii) $\forall(u,v)\in\mathcal{B}(\mathbb{N},\mathbb{R})^2\ ,\ (u-v)\in\mathcal{B}(\mathbb{N},\mathbb{R})$;

(iii) $\forall(u,v)\in\mathcal{B}(\mathbb{N},\mathbb{R})^2\ ,\ (u\times v)\in\mathcal{B}(\mathbb{N},\mathbb{R})$.

La propriété (i) est évidente car par exemple, $\forall n\in\mathbb{N}\ ,\ |1_{\mathbb{R}^{\mathbb{N}}}(n)|\leqslant 1$.

Montrons (ii) et (iii).
Soient $u=(u_n)_{n\in\mathbb{N}}$ et $v=(v_n)_{n\in\mathbb{N}}$ deux suites réelles bornées. Par définition, il existe $M\in\mathbb{R}^+$ et $M'\in\mathbb{R}^+$ tels que :

$$\forall n\in\mathbb{N}\ ,\ |u_n|\leqslant M\quad\text{et}\quad\forall n\in\mathbb{N}\ ,\ |v_n|\leqslant M'$$

Alors, pour tout entier $n\in\mathbb{N}$:

$$|(u-v)_n|=|u_n-v_n|\leqslant|u_n|+|v_n|\leqslant M+M'$$

Ce qui prouve que $u-v$ est bornée, c'est-à-dire $(u-v)\in\mathcal{B}(\mathbb{N},\mathbb{R})$. De même, pour tout $n\in\mathbb{N}$:

$$|(u\times v)_n|=|u_n\times v_n|=|u_n|\times|v_n|\leqslant M\times M'$$

Ce qui prouve que $u\times v\in\mathcal{B}(\mathbb{N},\mathbb{R})$.

• Montrons enfin que $\mathcal{B}(\mathbb{N},\mathbb{R})$ est stable par combinaisons linéaires.
En reprenant les mêmes notations que juste au-dessus et en fixant deux constantes réelles λ et μ, on a :

$$\begin{aligned}\forall n\in\mathbb{N}\ ,\ |(\lambda\cdot u+\mu\cdot v)_n| &= |\lambda\times u_n+\mu\times v_n|\\ &\leqslant |\lambda|\times|u_n|+|\mu|\times|v_n|\\ &\leqslant |\lambda|\times M+|\mu|\times M'\end{aligned}$$

Ce qui prouve que $(\lambda\cdot u+\mu\cdot v)$ est bornée.

⊠

Remarque : *en clair, on retient que cette proposition dit simplement que la somme de deux suites bornées est bornée et que le produit de deux suites bornées est encore une suite bornée.*

3.1.3 Suites extraites

Définition 3.1.3.1 Soit $(u_n)_{n\in\mathbb{N}} \in \mathbb{R}^{\mathbb{N}}$ une suite. On dit qu'une suite $(v_n)_{n\in\mathbb{N}}$ est une suite extraite de $(u_n)_{n\in\mathbb{N}}$ s'il existe une application $\varphi : \mathbb{N} \longrightarrow \mathbb{N}$ strictement croissante telle que :

$$\forall n \in \mathbb{N} \ , \ v_n = u_{\varphi(n)}$$

Exemple 3.1.3.2 (important) Les exemples classiques sont les suites extraites des termes d'indices pairs et impairs. Si $\varphi(n) = 2n$ et $\psi(n) = 2n + 1$ pour tout entier n, alors φ et ψ sont des applications strictement croissantes de $\mathbb{N}$ dans $\mathbb{N}$ et les suites $(u_{\varphi(n)})$ et $(u_{\psi(n)})$ sont donc des suites extraites de la suite $(u_n)_{n\in\mathbb{N}}$.

Exemple 3.1.3.3 La suite $(u_{4n^2})_{n\in\mathbb{N}}$ est une suite extraite de (u_n) mais aussi une suite extraite de la suite $(u_{n^2})_{n\in\mathbb{N}}$.

Exemple 3.1.3.4 En revanche, $(u_{n!})_{n\in\mathbb{N}}$ n'est pas une suite extraite de $(u_n)_{n\in\mathbb{N}}$ car l'application $n \longmapsto n!$ n'est pas strictement croissante de $\mathbb{N}$ dans $\mathbb{N}$ ($0! = 1!$). De même, $(u_{2E(\frac{n}{2})})_{n\in\mathbb{N}}$ n'est pas une suite extraite de $(u_n)_{n\in\mathbb{N}}$ car l'application $n \longmapsto 2E(\frac{n}{2})$ n'est pas strictement croissante.

Remarques : *on verra un peu plus loin l'utilisation des suites extraites mais,*

- *c'est un outil important pour montrer qu'une suite n'a pas de limite (voir le paragraphe 3) ;*
- *on verra dans ce chapitre (paragraphe 4) que pour une suite réelle bornée, il existe toujours au moins une suite extraite qui converge (théorème de Bolzano-Weierstrass) ;*
- *plus généralement, c'est une notion fondamentale en analyse qui permet par exemple de définir la notion de compacité (voir cours de mathématiques spéciales 1).*

Proposition 3.1.3.5 *Toute suite extraite d'une suite extraite de $(u_n)_{n\in\mathbb{N}}$ est encore une suite extraite de $(u_n)_{n\in\mathbb{N}}$.*

Preuve :

Soit $(v_n)_{n\in\mathbb{N}}$ une suite extraite de $(u_n)_{n\in\mathbb{N}}$ et soit $(w_n)_{n\in\mathbb{N}}$ une suite extraite de $(v_n)_{n\in\mathbb{N}}$. Par définition, il existe $\varphi : \mathbb{N} \longrightarrow \mathbb{N}$ strictement croissante telle que :

$$\forall n \in \mathbb{N} \ , \ v_n = u_{\varphi(n)}$$

De même, il existe $\psi : \mathbb{N} \longrightarrow \mathbb{N}$ strictement croissante telle que :

$$\forall n \in \mathbb{N} \ , \ w_n = v_{\psi(n)}$$

On a alors :

$$\forall n \in \mathbb{N} \ , \ w_n = v_{\psi(n)} = u_{\varphi(\psi(n))} = u_{(\varphi\circ\psi)(n)}$$

Par ailleurs, $\varphi \circ \psi$ est strictement croissante puisque c'est la composée de deux applications strictement croissantes.

⊠

Remarque : *ce qui est important, c'est de bien comprendre l'ordre de la composition. C'est $(u_{\varphi\circ\psi(n)})_{n\in\mathbb{N}}$ qui est une suite extraite de $(u_{\varphi(n)})_{n\in\mathbb{N}}$!*

3.2 Suites définies par une relation de récurrence

Proposition 3.2.0.1 *Soient E un ensemble, $a \in E$ et $(f_n)_{n\in\mathbb{N}}$ une famille d'applications de E dans E. Alors il existe une et une seule suite $(u_n)_{n\in\mathbb{N}}$ d'éléments de E vérifiant :*

$$u_0 = a \quad et \quad \forall n \in \mathbb{N} \ , \ u_{n+1} = f_n(u_n)$$

Une telle suite $(u_n)_{n\in\mathbb{N}}$ est appelée une suite récurrente d'ordre 1.

Preuve :

C'est évident. Pour le prouver formellement, il suffit de procéder par récurrence.

⊠

Remarque : *de façon plus générale, on peut définir une suite récurrente d'ordre p (avec $p \geqslant 1$) de la façon suivante. On se donne $(f_n)_{n\in\mathbb{N}}$ une famille d'applications de E^p dans E et $(a_0, \cdots, a_{p-1}) \in E^p$. Il existe une unique suite $(u_n)_{n\in\mathbb{N}}$ d'éléments de E vérifiant :*

$$\forall k \in [\![0, p-1]\!] \ , \ u_k = a_k \quad et \quad \forall n \in \mathbb{N} \ , \ u_{n+p} = f_n(u_n, u_{n+1}, \cdots, u_{n+p-1})$$

3.2.1 Suites arithmétiques et géométriques

Définition 3.2.1.1 On dit qu'une suite réelle ou complexe $(u_n)_{n\in\mathbb{N}}$ est une suite :

- arithmétique s'il existe $r \in \mathbb{C}$ tel que $\forall n \in \mathbb{N}$, $u_{n+1} = u_n + r$. Le nombre r est alors appelé la raison de la suite ;
- géométrique s'il existe $q \in \mathbb{C}$ tel que $\forall n \in \mathbb{N}$, $u_{n+1} = qu_n$. Le nombre q est alors appelé la raison de la suite.

⚠ **Attention :** pour montrer qu'une suite est géométrique, il ne faut pas calculer le rapport $\dfrac{u_{n+1}}{u_n}$ tant qu'on n'a pas démontré que $u_n \neq 0$!

On rappelle les expressions suivantes que vous devez impérativement connaître. Les démonstrations sont laissées en exercice.

Proposition 3.2.1.2 *Soit $(u_n)_{n\in\mathbb{N}}$ une suite réelle ou complexe.*

- *Si $(u_n)_{n\in\mathbb{N}}$ est arithmétique de raison $r \in \mathbb{C}$, et $p \in \mathbb{N}$, alors :*

$$\forall n \in \mathbb{N} \text{ , } u_n = u_p + (n-p)r$$

- *Si $(v_n)_{n\in\mathbb{N}}$ est géométrique de raison $q \in \mathbb{C}^\star$ et $p \in \mathbb{N}$, alors :*

$$\forall n \in \mathbb{N} \text{ , } v_n = q^{n-p}v_p$$

Exemple 3.2.1.3 On considère la suite définie par $u_0 \in]0, +\infty[$ et $\forall n \in \mathbb{N}$, $u_{n+1} = u_n^4$. On démontre par récurrence immédiate que pour tout entier n, $u_n > 0$ et on pose alors $v_n = \ln(u_n)$. Soit $n \in \mathbb{N}$; on a :

$$v_{n+1} = \ln(u_{n+1}) = 4\ln(u_n) = 4v_n$$

Par conséquent, $(v_n)_{n\in\mathbb{N}}$ est une suite géométrique et pour tout entier n, $v_n = v_0 \times 4^n$. Par suite,

$$\forall n \in \mathbb{N} \text{ , } u_n = e^{v_n} = u_0^{4^n}$$

Remarque : *sur ce dernier exemple, on aurait aussi pu conjecturer*[1] *l'expression de u_n et la démontrer par récurrence. Ceci étant dit, compte-tenu du temps nécessaire pour rédiger une récurrence convenablement, il est plus rapide d'appliquer la méthode de l'exemple.*

Exercice 3.2.1.4 On considère la suite $(u_n)_{n\in\mathbb{N}}$ définie par son premier terme $u_0 \in \mathbb{R}$ et la relation de récurrence :

$$\forall n \in \mathbb{N}\ ,\ u_{n+1} = -2u_n + 3$$

1. Montrer qu'il existe un unique $\ell \in \mathbb{R}$ (que vous déterminerez) tel que la suite $(v_n) = (u_n - \ell)$ soit géométrique.
2. En déduire l'expression de u_n en fonction de u_0 et de n pour tout entier $n \in \mathbb{N}$.

Exercice 3.2.1.5 On considère la suite $(u_n)_{n\in\mathbb{N}}$ définie par $u_0 = 2$, $u_1 = 5$ et la relation de récurrence :

$$\forall n \in \mathbb{N}\ ,\ u_{n+2} = 5u_{n+1} - 6u_n$$

1. Montrer qu'il existe (au moins) deux valeurs distinctes $\ell_1 \in \mathbb{R}$ et $\ell_2 \in \mathbb{R}$ telles que les suites $(u_{n+1} - \ell_i u_n)$ $(1 \leqslant i \leqslant 2)$ soient géométriques.
2. En déduire l'expression de u_n en fonction de n pour tout entier $n \in \mathbb{N}$.

On reverra un peu plus loin une suite $(u_n)_{n\in\mathbb{N}}$ de cette forme, on dispose directement de l'expression de u_n sans avoir à utiliser cette méthode « artificielle ».

3.2.2 Notations Σ et Π

Définition 3.2.2.1 Soit $(a_n)_{n\in\mathbb{N}}$ une suite de nombres réels ou complexes. On définit alors respectivement :

$$S_n = \sum_{k=0}^{n} a_k \quad \text{et} \quad P_n = \prod_{k=0}^{n} a_k$$

par les relations de récurrences suivantes :

$$\begin{cases} S_0 = a_0 \\ \forall n \in \mathbb{N}\ ,\ S_{n+1} = S_n + a_{n+1} \end{cases} \quad \text{et} \quad \begin{cases} P_0 = a_0 \\ \forall n \in \mathbb{N}\ ,\ P_{n+1} = a_{n+1} \times P_n \end{cases}$$

Remarque : *concrètement, $S_n = a_0 + a_1 + \cdots + a_n$ et $P_n = a_0 \times a_1 \times \cdots \times a_n$. Mais lorsqu'on rédige « proprement », on n'utilise pas les points de suspension ! Vous pouvez faire le raisonnement au brouillon avec « $\cdots$ », mais dans une copie, on les remplace par le symbole Σ (ou Π).*

1. c'est-à-dire deviner ou émettre une hypothèse.

Remarque importante : on peut de même définir une somme (ou un produit) à partir d'un certain rang. Par exemple, si $p \in \mathbb{N}^\star$ est donné, la suite (S'_n) définie par :

$$S'_n = \sum_{k=p}^{n} a_k \quad \text{est en réalité définie par :} \quad \begin{cases} \forall n \in [\![0, p-1]\!] \ , \ S'_n = 0 \\ S_p = a_p \\ \forall n \in \mathbb{N} \ , \ n \geqslant p \Longrightarrow S'_{n+1} = a_{n+1} + S'_n \end{cases}$$

Proposition 3.2.2.2 *Soient $(a_n)_{n\in\mathbb{N}}$ et $(b_n)_{n\in\mathbb{N}}$ deux suites de nombres réels ou complexes, $\lambda \in \mathbb{K}$ un scalaire et $p \in \mathbb{N}$ fixé. Alors, pour tout entier $n \geqslant p$:*

$$\sum_{k=p}^{n} \lambda a_k = \lambda \sum_{k=p}^{n} a_k \qquad et \qquad \sum_{k=p}^{n} (a_k + b_k) = \sum_{k=p}^{n} a_k + \sum_{p=0}^{n} b_k$$

De même,

$$\prod_{k=p}^{n} (\lambda a_k) = \lambda^{n+1-p} \prod_{k=p}^{n} a_k \qquad et \qquad \prod_{k=p}^{n} (a_k b_k) = \prod_{k=p}^{n} a_k \times \prod_{k=p}^{n} b_k$$

Preuve :

Montrons par exemple les propriétés du produit. On pose pour $n \in \mathbb{N}$:

$$A_n = \prod_{k=p}^{n} a_k \ ; \ B_n = \prod_{k=p}^{n} b_k \ ; \ P_n = \prod_{k=p}^{n} (\lambda a_k) \ ; \ Q_n = \prod_{k=p}^{n} (a_k \times b_k)$$

Montrons par récurrence sur $n \in \mathbb{N}$ (et $n \geqslant p$) que :

$$\forall n \geqslant p \ , \ P_n = \lambda^{n+1-p} A_n \ \text{ et } \ Q_n = A_n \times B_n$$

Initialisation :

Pour $n = p$, on a par définition des produits : $Q_p = a_p \times b_p = A_p \times B_p$ et $P_p = (\lambda a_p) = \lambda \times a_p = \lambda A_p = \lambda^{p+1-p} a_p$. Ce qui montre que la propriété est vraie au rang $n = p$.

Hérédité :

On suppose la propriété vraie au rang $n \geqslant p$: montrons qu'elle est vraie au rang $n + 1$. On a :

$$P_{n+1} = (\lambda a_{n+1}) \times P_n = (\lambda a_{n+1}) \times \lambda^{n+1-p} A_n = \lambda \times \lambda^{n+1-p} \times a_{n+1} \times A_n$$

d'où

$$P_{n+1} = \lambda^{n+2-p} \times A_{n+1}$$

et de même,

$$Q_{n+1} = (a_{n+1} \times b_{n+1}) \times Q_n = a_{n+1} \times b_{n+1} \times A_n \times B_n = A_{n+1} \times B_{n+1}$$

Ce qui montre que la propriété est vraie au rang $n+1$ et achève la récurrence.

⊠

Remarque : *on dit que l'opérateur somme est un opérateur linéaire (voir chapitre 4 pour la définition d'une application linéaire).*

Convention : on convient de poser :

$$\sum_{i \in \emptyset} a_i = 0 \quad \text{et} \quad \prod_{i \in \emptyset} a_i = 1$$

Remarque : *en particulier, on définit n factoriel, noté n!, par* $n! = \prod_{k=1}^{n} k$. *Avec la convention précédente, on a donc* $0! = 1$.

Technique de changement d'indice : le principe est simple, l'addition et la multiplication dans $\mathbb{C}$ sont commutatives. Par conséquent, on peut changer l'ordre des termes dans une somme finie (ou un produit fini) sans modifier la valeur de la somme (ou du produit). Concrètement, cela signifie qu'on peut effectuer des changements d'indices dans les sommes, à condition que ces changements soient bijectifs (pour éviter d'oublier des termes (surjectivité) ou d'en compter en double, triple... (injectivité)). Par ailleurs, la variable « k » dans la somme est une variable « muette » : c'est-à-dire qu'on peut remplacer « k » par n'importe quel symbole (qui n'est pas déjà utilisé). Donnons quelques exemples.

Exemple 3.2.2.3 Soit pour $n \in \mathbb{N}^\star$, $S_n = \sum_{k=1}^{n} k$. Si on pose pour $k \in [\![1, n]\!]$, $i = n - k$, alors lorsque k varie entre 1 et n, i varie entre 0 et $n-1$. De plus, il est clair que $k \longmapsto n-k$ est une bijection de $[\![1, n]\!]$ dans $[\![0, n-1]\!]$. Par conséquent,

$$\sum_{k=1}^{n} k = \sum_{i=0}^{n-1} (n-i) = \sum_{k=0}^{n-1} (n-k)$$

Dans la pratique, quand le changement d'indice est « simple », on fait simplement le changement d'indice sans écrire toutes les explications.

Exercice 3.2.2.4 Prouver directement que $\sum_{k=1}^{n} k = \dfrac{n(n+1)}{2}$ en faisant le changement d'indice $i = n - k$.

Exemple 3.2.2.5 De la même façon, on a pour tout entier n et tout réel x :

$$\sum_{k=0}^{n} \cos((k+1)x) = \sum_{p=1}^{n+1} \cos(px) = \sum_{k=1}^{n+1} \cos(kx)$$

Il y a un cas particulier très important, celui des sommes télescopiques.

Proposition 3.2.2.6 *Soit $(a_n)_{n\in\mathbb{N}}$ une suite d'éléments de $E \subset \mathbb{C}$. Alors pour tout entier n,*

$$\sum_{k=0}^{n} (a_{k+1} - a_k) = a_{n+1} - a_0$$

De telles sommes sont appelées des sommes (ou séries) télescopiques.

Preuve :

Soit $n \in \mathbb{N}$. On a alors :

$$\begin{aligned}
\sum_{k=0}^{n} (a_{k+1} - a_k) &= \sum_{k=0}^{n} a_{k+1} - \sum_{k=0}^{n} a_k \quad \text{(linéarité de la somme)} \\
&= \sum_{i=1}^{n+1} a_i - \sum_{k=0}^{n} a_k \quad \text{(changement d'indice } i = k+1\text{)} \\
&= \sum_{k=1}^{n+1} a_k - \sum_{k=0}^{n} a_k \quad \text{(l'indice est une variable muette)} \\
&= a_{n+1} + \sum_{k=1}^{n} a_k - \sum_{k=1}^{n} a_k - a_0 \\
&= a_{n+1} - a_0
\end{aligned}$$

⊠

⚠ **Attention :** on ne peut pas faire n'importe quel changement d'indice. Par exemple, dans la somme $\sum_{k=0}^{n} 2^{k^2}$, on ne peut pas poser $i = k^2$ et obtenir $\sum_{i=0}^{n^2} 2^i$. Pourquoi ?

Exercice 3.2.2.7 Calculer pour $n \geqslant 1$ la somme : $S_n = \sum_{k=1}^{n} \frac{1}{k(k+1)}$.

Exercice 3.2.2.8 Calculer pour $n \geqslant 1$ la somme : $S_n = \sum_{k=0}^{n} \cos\left(k + \frac{1}{2}\right)$ en utilisant une somme télescopique.

On peut manipuler de la même façon les sommes finies avec deux indices. On peut regrouper ou permuter les termes de n'importe quelle manière tant qu'on ne rajoute pas de terme et qu'on n'en supprime pas.

Exercice 3.2.2.9 Calculer pour $n \geqslant 1$ et $x \in \mathbb{R}$, $T_n = \sum_{1 \leqslant i,j \leqslant n} x^{i+j}$.

Proposition 3.2.2.10 *Soit $(u_n)_{n\in\mathbb{N}}$ une suite arithmétique de raison r. Alors pour tout $p, n \in \mathbb{N}$ avec $p \leqslant n$:*

$$\sum_{k=p}^{n} u_k = (n+1-p) \times \frac{u_p + u_n}{2}$$

Soit $(v_n)_{n\in\mathbb{N}}$ une suite géométrique de raison $q \neq 1$, alors pour tout $p, n \in \mathbb{N}$ tels que $p \leqslant n$:

$$\sum_{k=p}^{n} v_k = \frac{v_p - v_{n+1}}{1-q}$$

Preuve :

Avec les hypothèses de la proposition, on a :

$$\begin{aligned}
2\sum_{k=p}^{n} u_k &= \sum_{k=p}^{n} (u_p + (k-p)r) + \sum_{k=p}^{n} (u_n + (k-n)r) \\
&= \sum_{k=p}^{n} (u_p + u_n) + r\left(\sum_{k=p}^{n}(k-p) - \sum_{k=p}^{n}(n-k)\right) \\
&= (n+p-1) \times (u_p + u_n) + r\left(\sum_{i=0}^{n-p} i - \sum_{j=0}^{n-p} j\right) \\
&= (n+p-1) \times (u_p + u_n)
\end{aligned}$$

Par ailleurs,

$$\begin{aligned}
(1-q)\sum_{k=p}^{n} v_k &= \sum_{k=p}^{n} v_k - \sum_{k=p}^{n} q v_k \\
&= \sum_{k=p}^{n} v_k - \sum_{k=p}^{n} v_{k+1} \\
&= v_p - v_{n+1}
\end{aligned}$$

(on reconnaît une somme télescopique dans la dernière égalité). ⊠

Remarque : *on peut retenir ces formules à l'aide des phrases suivantes :*

- *pour la somme des termes consécutifs d'une suite arithmétique : « moyenne du premier et du dernier terme de la somme multiplié par le nombre de termes dans la somme » ;*
- *pour la somme des termes consécutifs d'une suite géométrique : « premier terme qui est dans la somme moins premier terme qui n'est pas dans la somme, le tout divisé par* 1 *moins la raison ».*

Cas particuliers usuels : avec les notations précédentes et toujours si $q \neq 1$,

$$\sum_{k=0}^{n} u_k = (n+1)u_0 + \frac{n(n+1)}{2}r \quad \text{et} \quad \sum_{k=0}^{n} q^k = \frac{1-q^{n+1}}{1-q}$$

3.2.3 Suites récurrentes linéaires d'ordre 2 à coefficients constants

Dans tout ce paragraphe, $a, b, c \in \mathbb{K}$ et $a \neq 0$ (où $\mathbb{K} = \mathbb{R}$ ou $\mathbb{K} = \mathbb{C}$) et $(d_n)_{n\in\mathbb{N}}$ est une suite donnée. On s'intéresse aux suites $(u_n)_{n\in\mathbb{N}}$ vérifiant la relation :

$$(E) : \ \forall n \in \mathbb{N} \ , \ au_{n+2} + bu_{n+1} + cu_n = d_n$$

On note tout comme pour les équations différentielles :

$$(E_H) : \ \forall n \in \mathbb{N} \ , \ au_{n+2} + bu_{n+1} + cu_n = 0$$

Proposition 3.2.3.1 *Soit $\mathcal{S}$ (respectivement $\mathcal{S}_H$) l'ensemble des suites vérifiant la relation (E) (respectivement (E_H)). Alors :*

(i) S_H est non vide et stable par combinaisons linéaires :

$$\forall (u_n)_{n\in\mathbb{N}}, (v_n)_{n\in\mathbb{N}} \in \mathcal{S}_H \ , \ \forall \lambda, \mu \in \mathbb{K} \ , \ (\lambda u_n + \mu v_n) \in \mathcal{S}_H$$

En particulier, S_H est un groupe abélien.

(ii) Si $(v_n)_{n\in\mathbb{N}}$ est une solution de (E), alors $\mathcal{S} = \{(v_n + u_n) \mid (u_n)_{n\in\mathbb{N}} \in \mathcal{S}_H\}$.

Remarque : *j'espère que vous remarquez l'analogie avec les équations différentielles linéaires du second ordre à coefficients constants. Si vous vous souvenez du cours sur les équations différentielles, vous avez vu que ce théorème de structure des solutions est valable pour toute équation « linéaire ».*

L'ensemble des solutions de l'équation homogène est toujours un « espace-vectoriel » et l'ensemble des solutions de l'équation linéaire est soit vide, soit un « espace affine ». On reverra tout cela en détails dans le chapitre suivant.

Preuve de la proposition :

• Montrons (i).
Il est clair que la suite constante égale à 0 est solution de (E_H). Par suite, $\mathcal{S}_H \neq \emptyset$.
Par ailleurs, soient $(u_n)_{n\in\mathbb{N}}, (v_n)_{n\in\mathbb{N}} \in \mathcal{S}_H$ et λ, μ deux nombres dans $\mathbb{K}$. On considère la suite : $(w_n)_{n\in\mathbb{N}} = \lambda(u_n)_{n\in\mathbb{N}} + \mu(v_n)_{n\in\mathbb{N}}$, c'est-à-dire la suite définie par :

$$\forall n \in \mathbb{N}\ ,\ w_n = \lambda u_n + \mu v_n$$

Soit $n \in \mathbb{N}$. Notons $x_n = aw_{n+2} + bw_{n+1} + cw_n$. On a :

$$\begin{aligned} x_n &= a(\lambda u_{n+2} + \mu v_{n+2}) + b(\lambda u_{n+1} + \mu v_{n+1}) + c(\lambda u_n + \mu v_n) \\ &= \lambda(au_{n+2} + bu_{n+1} + cu_n) \ + \ \mu(av_{n+2} + bv_{n+1} + cv_n) \\ &= \lambda \times 0 + \mu \times 0 \quad (\text{car } (u_n)_{n\in\mathbb{N}}, (v_n)_{n\in\mathbb{N}} \in \mathcal{S}_H) \\ &= 0 \end{aligned}$$

Par conséquent, $(w_n)_{n\in\mathbb{N}} \in \mathcal{S}_H$.

• Montrons (ii).
Soit $(v_n)_{n\in\mathbb{N}}$ une solution de (E). Soit $(x_n)_{n\in\mathbb{N}}$ une suite quelconque de nombres dans $\mathbb{K}$. On note $(z_n)_{n\in\mathbb{N}} = (x_n)_{n\in\mathbb{N}} - (v_n)_{n\in\mathbb{N}}$. Alors :

$$\begin{aligned} (x_n)_{n\in\mathbb{N}} \in \mathcal{S} &\iff \forall n \in \mathbb{N}\ ,\ ax_{n+2} + bx_{n+1} + cx_n = d_n \\ &\iff \forall n \in \mathbb{N}\ ,\ ax_{n+2} + bx_{n+1} + cx_n = av_{n+2} + bv_{n+1} + cv_n \\ &\iff \forall n \in \mathbb{N}\ ,\ az_{n+2} + bz_{n+1} + cz_n = 0 \\ &\iff (z_n)_{n\in\mathbb{N}} \in \mathcal{S}_H \end{aligned}$$

Ce qui prouve le second point.

⊠

Remarque : *en clair, cela veut dire que pour déterminer les solutions de (E), on procède comme pour les équations différentielles :*

- *on commence par résoudre l'équation homogène associée ;*
- *puis, on détermine une solution particulière ;*
- *enfin, les solutions s'obtiennent en prenant la solution particulière trouvée et en lui ajoutant les solutions de (E_H).*

Il reste maintenant à déterminer les solutions de l'équation homogène associée.

Lemme 3.2.3.2 *L'application φ suivante :*

$$\begin{array}{ccc} \mathcal{S}_H & \xrightarrow{\varphi} & \mathbb{K}^2 \\ (u_n) & \longmapsto & (u_0, u_1) \end{array}$$

est une application linéaire et bijective. En particulier, φ est un isomorphisme de groupes additifs.

Preuve :

• Montrons pour commencer que φ est linéaire.

Soient $(u_n)_{n\in\mathbb{N}}, (v_n)_{n\in\mathbb{N}} \in \mathcal{S}_H$ et $\lambda, \mu \in \mathbb{K}$. Alors :

$$\begin{aligned} \varphi\left(\lambda(u_n)_{n\in\mathbb{N}} + \mu(v_n)_{n\in\mathbb{N}}\right) &= (\lambda u_0 + \mu v_0, \lambda u_1 + \mu v_1) \\ &= \lambda(u_0, u_1) + \mu(v_0, v_1) \\ &= \lambda\varphi((u_n)_{n\in\mathbb{N}}) + \mu\varphi((v_n)_{n\in\mathbb{N}}) \end{aligned}$$

Par conséquent, φ est une application linéaire.

• Montrons à présent que φ est bijective.

∗ Injectivité

Soient $(u_n)_{n\in\mathbb{N}}, (v_n)_{n\in\mathbb{N}} \in \mathcal{S}_H$ telles que $\varphi((u_n)_{n\in\mathbb{N}}) = \varphi((v_n)_{n\in\mathbb{N}})$, c'est-à-dire $u_0 = v_0$ et $u_1 = v_1$. On montre alors, de façon immédiate, par récurrence double que pour tout entier n, $u_n = v_n$, c'est-à-dire $(u_n)_{n\in\mathbb{N}} = (v_n)_{n\in\mathbb{N}}$.
Ce qui prouve que φ est injective.

∗ Surjectivité

Soit $(\alpha, \beta) \in \mathbb{K}^2$. On rappelle que par hypothèse, $a \neq 0$.
On définit alors la suite $(u_n)_{n\in\mathbb{N}}$ par :

$$u_0 = \alpha \quad \text{et} \quad u_1 = \beta \quad \text{et} \quad \forall n \in \mathbb{N}\ ,\ u_{n+2} = -\frac{b}{a}u_{n+1} - \frac{c}{a}u_n$$

Il est clair que cette relation définit bien une suite $(u_n)_{n\in\mathbb{N}}$ qui vérifie la relation (E_H), c'est-à-dire $(u_n)_{n\in\mathbb{N}} \in \mathcal{S}_H$ et par construction,

$$\varphi((u_n)_{n\in\mathbb{N}}) = (\alpha, \beta)$$

Ceci prouve que φ est surjective.

⊠

Corollaire 3.2.3.3 *L'ensemble $\mathcal{S}$ est toujours non vide et l'application ψ :*

$$\begin{array}{ccc} \mathcal{S} & \xrightarrow{\psi} & \mathbb{K}^2 \\ (u_n) & \longmapsto & (u_0, u_1) \end{array}$$

est une application bijective.

Preuve :

• Pour commencer, on définit la suite $(v_n)_{n\in\mathbb{N}}$ par : $v_0 = v_1 = 0$ et pour tout entier naturel n, $v_{n+2} = -\frac{b}{a}v_{n+1} - \frac{c}{a}v_n - \frac{1}{a}d_n$.
Il est clair que ceci définit bien une suite $(v_n)_{n\in\mathbb{N}}$ et que $(v_n)_{n\in\mathbb{N}} \in \mathcal{S}$. Par suite, $\mathcal{S} \neq \emptyset$.

• Montrons à présent que ψ est bijective. Pour cela, soit $(\alpha, \beta) \in \mathbb{K}^2$: on montre que l'équation $\psi((u_n)_{n\in\mathbb{N}}) = (\alpha, \beta)$ admet une unique solution $(u_n)_{n\in\mathbb{N}} \in \mathcal{S}$.
Soit $(u_n)_{n\in\mathbb{N}} \in \mathcal{S}$. La suite $(v_n)_{n\in\mathbb{N}}$ précédente appartient à $\mathcal{S}$: d'après le théorème de structure des solutions, il existe $(x_n)_{n\in\mathbb{N}} \in \mathcal{S}_H$ telle que $(u_n)_{n\in\mathbb{N}} = (v_n)_{n\in\mathbb{N}} + (x_n)_{n\in\mathbb{N}}$ et on a alors :

$$\begin{array}{rcl} \psi((u_n)_{n\in\mathbb{N}}) = (\alpha, \beta) & \iff & (x_0, x_1) = (\alpha - v_0, \beta - v_1) \\ & \iff & \varphi((x_n)_{n\in\mathbb{N}}) = (\alpha - v_0, \beta - v_1) \\ & \iff & (x_n)_{n\in\mathbb{N}} = \varphi^{-1}(\alpha - v_0, \beta - v_1) \\ & \iff & (u_n)_{n\in\mathbb{N}} = (v_n)_{n\in\mathbb{N}} + \varphi^{-1}(\alpha - v_0, \beta - v_1) \end{array}$$

prouvant ainsi que pour tout $(\alpha, \beta) \in \mathbb{K}^2$, l'équation $\psi((u_n)_{n\in\mathbb{N}}) = (\alpha, \beta)$ admet une unique solution dans $\mathcal{S}$, c'est-à-dire que ψ est bijective.

⊠

⚠ **Attention :** en revanche, l'application ψ n'est pas une application linéaire ou un morphisme de groupes ! L'ensemble $\mathcal{S}$ n'est en général pas un groupe pour l'addition (sauf si $0 \in \mathcal{S}$).

De façon analogue aux équations différentielles, on définit le polynôme caractéristique (ou équation caractéristique).

Définition 3.2.3.4 L'équation $P(z) = 0$ avec $P(z) = az^2 + bz + c$ est appelée équation caractéristique associée à (E). P est appelé le polynôme caractéristique associé.

On va maintenant déterminer explicitement les solutions de (E_H). Pour éviter un problème technique d'écriture des solutions dans un cas très particulier, on va éliminer le cas $c = 0$. Lorsque $c = 0$, (E_H) s'écrit $au_{n+2} + bu_{n+1} = 0$ pour tout entier $n \in \mathbb{N}$. On constate alors que la suite $(u_{n+1})_{n\in\mathbb{N}}$ est géométrique de raison $q = \frac{-b}{a}$. Il s'ensuit que pour $n \in \mathbb{N}$, $u_{n+1} = q^n u_1$ et il n'y a aucune condition sur u_0. On peut donc donner explicitement la suite, sans avoir à utiliser le polynôme caractéristique.

Proposition 3.2.3.5 *Pour tout $a, b, c \in \mathbb{K}$ avec $a \neq 0$ et $c \neq 0$. $\mathcal{S}_H$ est un plan vectoriel. Plus précisément,*

- *Si le polynôme P admet deux racines distinctes r_1 et r_2 ($\Delta \neq 0$), alors : $((r_1^n)_{n\in\mathbb{N}}, (r_2^n)_{n\in\mathbb{N}})$ est une base de $\mathcal{S}_H$. Autrement dit,*

$$(u_n) \in \mathcal{S}_H \iff \exists!(\lambda, \mu) \in \mathbb{K}^2 \ , \ \forall n \in \mathbb{N} \ , \ u_n = \lambda r_1^n + \mu r_2^n$$

- *Si P admet une racine double $r_0 \neq 0$, alors $((r_0^n)_{n\in\mathbb{N}}, (nr_0^n)_{n\in\mathbb{N}})$ est une base de $\mathcal{S}_H$. Autrement dit,*

$$(u_n) \in \mathcal{S}_H \iff \exists!(\lambda, \mu) \in \mathbb{K}^2 \ , \ \forall n \in \mathbb{N} \ , \ u_n = \lambda r_0^n + \mu n r_0^n$$

Preuve :

Tout d'abord, on commence par remarquer que si r est une racine de P, alors $(r^n)_{n\in\mathbb{N}} \in \mathcal{S}_H$. En effet, pour tout entier n, on a :

$$ar^{n+2} + br^{n+1} + cr^n = r^n \times P(r) = 0$$

- On suppose que P admet deux racines distinctes r_1 et r_2.
  - Montrons $\Longleftarrow$
    D'après ce qui précède, $(r_1^n)_{n\in\mathbb{N}} \in \mathcal{S}_H$ et $(r_2^n)_{n\in\mathbb{N}} \in \mathcal{S}_H$. Alors, d'après la proposition 3.2.3.1 (la structure de l'ensemble $\mathcal{S}_H$), on en déduit que pour tout $(\lambda, \mu) \in \mathbb{K}^2$, $\lambda(r_1^n)_{n\in\mathbb{N}} + \mu(r_2^n)_{n\in\mathbb{N}} \in \mathcal{S}_H$.
  - Montrons l'implication directe.
    Soit $(u_n)_{n\in\mathbb{N}} \in \mathcal{S}_H$. Le système suivant (d'inconnues λ et μ)

$$\begin{cases} u_0 &= \lambda + \mu \\ u_1 &= \lambda r_1 + \mu r_2 \end{cases}$$

    a pour déterminant $r_2 - r_1 \neq 0$ et admet donc une unique solution (λ_0, μ_0) [1]. Considérons alors la suite $(v_n)_{n\in\mathbb{N}}$ définie pour tout

1. si vous n'êtes plus familier avec le déterminant du système, vous pouvez résoudre explicitement.

entier n par : $v_n = \lambda_0 r_1^n + \mu_0 r_2^n$. Alors d'une part, $(v_n)_{n\in\mathbb{N}} \in \mathcal{S}_H$ (d'après l'implication réciproque déjà prouvée) et d'autre part :

$$\varphi((u_n)_{n\in\mathbb{N}}) = \varphi((v_n)_{n\in\mathbb{N}})$$

c'est-à-dire $(u_n)_{n\in\mathbb{N}} = (v_n)_{n\in\mathbb{N}}$ (puisque φ est injective). Ce qui prouve l'implication directe.

• La démonstration pour le second cas est presque identique à quelques différences près :

∗ si on pose pour $n \in \mathbb{N}$, $s_n = nr_0^n$, alors pour tout entier $n \in \mathbb{N}$:

$$\begin{aligned} as_{n+2} + bs_{n+1} + cs_n &= (n+2)r_0^n a r_0^2 + (n+1)r_0^n b r_0 + cnr_0^n \\ &= nr_0^n(ar_0^2 + br_0 + c) + r_0^n(2ar_0 + b) \\ &= nr_0^n P(r_0) + r_0^n P'(r_0) \\ &= 0 \end{aligned}$$

(car r_0 est une racine double donc $P(r_0) = P'(r_0) = 0$).

∗ Ensuite, pour $(u_n)_{n\in\mathbb{N}} \in \mathcal{S}_H$, le système (d'inconnues λ et μ) devient :

$$\left\{ \begin{array}{rcl} u_0 &=& \lambda \\ u_1 &=& \lambda r_0 + \mu r_0 \end{array} \right.$$

qui admet bien une unique solution (car $r_0 \neq 0$).

⊠

Exemple 3.2.3.6 On considère la suite $(u_n)_{n\in\mathbb{N}}$ définie par $u_0 = 1$, $u_1 = -2$ et la relation de récurrence :

$$\forall n \in \mathbb{N}\ ,\ u_{n+2} = 4u_{n+1} - 4u_n$$

Le polynôme caractéristique associé est $P = X^2 - 4X + 4$. Ce polynôme admet une racine double $r = 2$. On en déduit qu'il existe $(\lambda, \mu) \in \mathbb{R}^2$ (qui est unique) tel que :

$$\forall n \in \mathbb{N}\ ,\ u_n = (\lambda n + \mu) \times 2^n$$

Or, $u_0 = 1$ et $u_1 = -2$ donc en remplaçant, on obtient $\mu = 1$ et $\lambda + \mu = -1$, c'est-à-dire $\lambda = -2$. Par conséquent,

$$\forall n \in \mathbb{N}\ ,\ u_n = (1 - 2n)2^n$$

Lorsqu'on cherche une « solution particulière », on peut utiliser les mêmes méthodes que pour les équations différentielles lorsque le second membre est de la forme $Q(n)r^n$ avec Q un polynôme et r une constante.

Exemple 3.2.3.7 Déterminons l'ensemble $\mathcal{S}$ de toutes les suites réelles telles que :

$$\forall n \in \mathbb{N}\ ,\ u_{n+2} - 4u_{n+1} + 4u_n = 2^n + n3^n$$

On vient de prouver que les solutions de l'équation homogène associée sont de la forme $((\lambda n + \mu)2^n)_{n\in\mathbb{N}}$. Il reste donc à trouver une solution particulière.

- Pour la suite $(n3^n)_{n\in\mathbb{N}}$, $r = 3$ n'est pas une racine du polynôme caractéristique. On va donc chercher une solution sous la forme $(v_n)_{n\in\mathbb{N}} = ((\alpha n + \beta)3^n)_{n\in\mathbb{N}}$ avec α, β deux réels. Soit $n \in \mathbb{N}$.

  $$v_{n+2} - 4v_{n+1} + 4v_n = 3^n\left(\alpha n + (6\alpha + \beta)\right)$$

  Par suite,

  $$\begin{aligned} \forall n \in \mathbb{N}\ ,\ v_{n+2} - 4v_{n+1} + 4v_n = n3^n &\iff \forall n \in \mathbb{N}\ ,\ \alpha n + (6\alpha + \beta) = n \\ &\iff \begin{cases} \alpha = 1 \\ \beta = -6 \end{cases} \end{aligned}$$

  On en déduit qu'une solution particulière pour le second membre $(n3^n)_{n\in\mathbb{N}}$ est définie par :

  $$\forall n \in \mathbb{N}\ ,\ v_n = (n-6) \times 3^n$$

- Pour la suite $(2^n)_{n\in\mathbb{N}}$, $r = 2$ est une racine double du polynôme caractéristique. On cherche donc une solution $(w_n)_{n\in\mathbb{N}}$ sous la forme $(w_n) = (\gamma n^2 2^n)$ avec $\gamma \in \mathbb{R}$. Or, pour tout entier n,

  $$w_{n+2} - 4w_{n+1} + 4w_n = \gamma 2^n\left(4(n+2)^2 - 8(n+1)^2 + 4n^2\right) = 8\gamma 2^n$$

  Il s'ensuit qu'en choisissant $\gamma = \frac{1}{8}$, on obtient une solution particulière.

Ainsi, on en déduit que $(u_n)_{n\in\mathbb{N}} \in \mathcal{S}$ si et seulement si il existe $(\lambda, \mu) \in \mathbb{R}^2$ tel que :

$$\forall n \in \mathbb{N}\ ,\ u_n = \frac{n^2}{8}2^n + (n-6)3^n + (\lambda n + \mu)2^n$$

Exercice 3.2.3.8 Déterminer l'ensemble des suites réelles vérifiant :

$$\forall n \in \mathbb{N}\ ,\ u_{n+2} - 5u_{n+1} + 6u_n = 1 + n + 3^n$$

Exercice 3.2.3.9 Déterminer la suite complexe vérifiant : $u_0 = u_1 = 1 + i$, et pour tout entier n :

$$u_{n+2} + (i-5)u_{n+1} + (8-4i)u_n = 0$$

Corollaire 3.2.3.10 *On suppose cette fois que $\mathbb{K} = \mathbb{R}$, c'est-à-dire $(a, b, c) \in \mathbb{R}^3$ et $a \neq 0$. Si P n'a pas de racines réelles (c'est-à-dire $\Delta < 0$), soit $r_1 \in \mathbb{C}$ une racine complexe de P. On écrit $r_1 = re^{i\theta}$ avec $r > 0$ et $\theta \in \mathbb{R}$. Alors :*

$$(u_n)_{n\in\mathbb{N}} \in \mathcal{S}_H \iff \exists!(A, B) \in \mathbb{R}^2 \ , \ \forall n \in \mathbb{N} \ , \ u_n = r^n \left(A\cos(n\theta) + B\sin(n\theta)\right)$$

Preuve :

Si $\Delta < 0$, alors, avec les notations du corollaire, P admet deux racines complexes r_1 et $\overline{r_1}$. On a donc d'après ce qui précède, en notant (A) la propriété : $(u_n)_{n\in\mathbb{N}}$ est solution de (E_H) et $(u_n)_{n\in\mathbb{N}}$ est une suite réelle, on a :

$$\begin{aligned}
(A) &\iff \begin{cases} \exists!(\lambda, \mu) \in \mathbb{C}^2 \ , \ \forall n \in \mathbb{N} \ , \ u_n = \lambda r_1^n + \mu \overline{r_1}^n \\ \forall n \in \mathbb{N} \ , \ u_n = \overline{u_n} \end{cases} \\
&\iff \begin{cases} \exists!(\lambda, \mu) \in \mathbb{C}^2 \ , \ \forall n \in \mathbb{N} \ , \ u_n = \lambda r_1^n + \mu \overline{r_1}^n \\ \mu = \overline{\lambda} \end{cases} \\
&\iff \exists!\lambda \in \mathbb{C} \ , \ \forall n \in \mathbb{N} \ , \ u_n = \lambda r_1^n + \overline{\lambda}\overline{r_1}^n \\
&\iff \exists!\lambda \in \mathbb{C} \ , \ u_n = 2\Re e\left(\lambda r^n e^{in\theta}\right) \\
&\iff \exists!(A, B) \in \mathbb{R}^2 \ , \ \forall n \in \mathbb{N} \ , \ u_n = r^n \left(A\cos(n\theta) + B\sin(n\theta)\right)
\end{aligned}$$

⊠

⚠ **Attention :** il ne faut pas confondre ce résultat avec celui des équations différentielles linéaires à coefficients constants ! Si le polynôme caractéristique P a un discriminant strictement négatif et si r_1 est une racine complexe du polynôme, alors en notant :

$$r_1 = \alpha + i\beta = re^{i\theta}$$

- les solutions (réelles) de $ay'' + by' + cy = 0$ sont les fonctions définies sur $\mathbb{R}$ par :

$$\forall t \in \mathbb{R} \ , \ y(t) = e^{\alpha t}\left(A\cos(\beta t) + B\sin(\beta t)\right) \qquad \text{avec } (A, B) \in \mathbb{R}^2$$

- les solutions de $\forall n \in \mathbb{N} \ , \ au_{n+2} + bu_{n+1} + cu_n = 0$ sont les suites définies par :

$$\forall n \in \mathbb{N} \ , \ u_n = r^n \left(A\cos(n\theta) + B\sin(n\theta)\right) \qquad \text{avec } (A, B) \in \mathbb{R}^2$$

Dans le premier cas, les solutions sont obtenues en prenant la forme algébrique de r_1 et dans le second, elles sont obtenues en prenant la forme exponentielle de r_1.

Exercice 3.2.3.11 Déterminer la suite $(u_n)_{n\in\mathbb{N}}$ vérifiant $u_0 = 1$, $u_1 = \sqrt{3} - 1$ et :

$$\forall n \in \mathbb{N} \ , \ u_{n+2} + 2u_{n+1} + 4u_n = 0$$

3.3 Limite d'une suite

3.3.1 Convergence vers un réel ℓ : définition et propriétés

Vous avez déjà appris de façon informelle la notion de limite. Pour une suite $(u_n)_{n\in\mathbb{N}}$, dire que la limite de la suite est ℓ signifie que « tous les termes de la suite deviennent aussi proche que l'on veut de ℓ à partir d'un certain rang ». Ceci signifie que la « distance » entre u_n et ℓ devient aussi petite que l'on veut. Or, dans $\mathbb{R}$, la « distance » entre deux nombres réels x et y est donnée par $|x-y|$. Le « aussi proche » que l'on veut signifie que quel que soit l'écart (que l'on va noter ε) strictement positif, à partir d'un certain rang, tous les termes vérifient $|u_n - \ell| \leqslant \varepsilon$. Ceci nous amène à poser une définition un peu plus formelle de la limite.

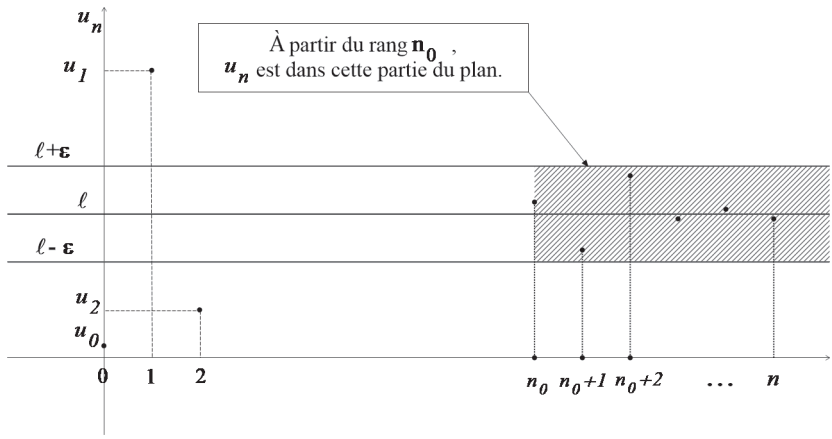
Définition 3.3.1.1 Soit $(u_n)_{n\in\mathbb{N}}$ une suite réelle et $\ell \in \mathbb{R}$. On dit que $(u_n)_{n\in\mathbb{N}}$ admet ℓ pour limite si :

$$\forall \varepsilon > 0 \ , \ \exists N \in \mathbb{N} \ , \ \forall n \in \mathbb{N} \ , \ (n \geqslant N \Longrightarrow |u_n - \ell| \leqslant \varepsilon \,)$$

Remarque importante : une autre écriture possible est :

$$(u_n)_{n\in\mathbb{N}} \text{ admet } \ell \text{ pour limite} \iff \forall \varepsilon > 0 \ , \ \exists N \in \mathbb{N} \ , \ \forall n \geqslant N \ , \ |u_n - \ell| \leqslant \varepsilon$$

On utilise souvent cette écriture qui sous-entend que $n \in \mathbb{N}$, plutôt que la définition précédente. Graphiquement, $(u_n)_{n\in\mathbb{N}}$ admet ℓ pour limite se traduit ainsi :



Théorème 3.3.1.2 (Définition) *On dit qu'une suite $(u_n)_{n\in\mathbb{N}}$ est convergente (ou admet une limite finie) s'il existe un réel ℓ tel que $(u_n)_{n\in\mathbb{N}}$ admet ℓ pour limite.*
Dans ce cas, le réel ℓ est unique et est appelé la limite de la suite. On note alors $\ell = \lim\limits_{n\to+\infty} u_n$ et on dit que la suite $(u_n)_{n\in\mathbb{N}}$ converge vers ℓ.

Preuve :

On suppose que $(u_n)_{n\in\mathbb{N}}$ admet $\ell \in \mathbb{R}$ et $\ell' \in \mathbb{R}$ pour limites. Montrons que $\ell = \ell'$.

Soit $\varepsilon > 0$. Par hypothèse, $(u_n)_{n\in\mathbb{N}}$ admet ℓ pour limite donc, par définition :

$$\exists n_1 \in \mathbb{N} \ , \ \forall n \geqslant n_1 \ , \ |u_n - \ell| \leqslant \frac{\varepsilon}{2}$$

Soit un tel entier n_1. De même, $(u_n)_{n\in\mathbb{N}}$ admet ℓ' pour limite donc :

$$\exists n_2 \in \mathbb{N} \ , \ \forall n \geqslant n_2 \ , \ |u_n - \ell'| \leqslant \frac{\varepsilon}{2}$$

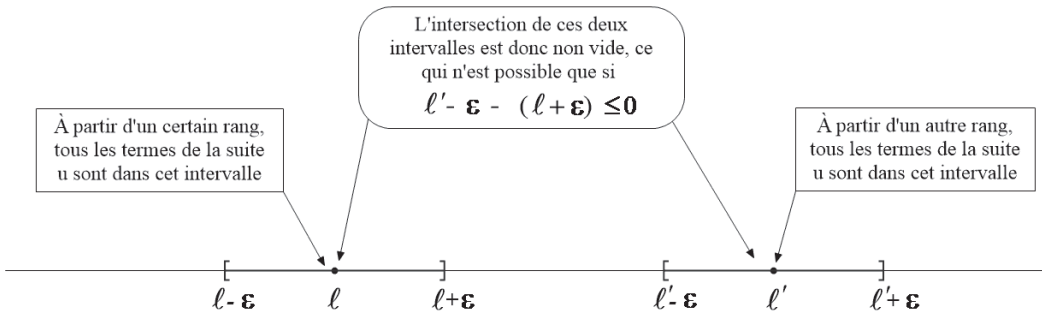
Soit un tel entier n_2. On pose alors [1] $N = \max(n_1, n_2)$. Soit $n \geqslant N$; alors $n \geqslant n_1$ et $n \geqslant n_2$ et on a donc :

$$\begin{aligned} |\ell - \ell'| &= |\ell - u_n + u_n - \ell'| \\ &\leqslant |\ell - u_n| + |u_n - \ell'| \\ &\leqslant \varepsilon \end{aligned}$$

Ainsi, on a montré que $\forall \varepsilon > 0 \ , \ |\ell - \ell'| \leqslant \varepsilon$, c'est-à-dire $|\ell - \ell'| = 0$, soit encore $\ell = \ell'$.

⊠

Remarque : *en fait, l'idée de la démonstration est très simple. Si $(u_n)_{n\in\mathbb{N}}$ admet deux limites ℓ et ℓ' avec $\ell \leqslant \ell'$, alors pour tout $\varepsilon > 0$:*


L'intersection de ces deux intervalles est donc non vide, ce qui n'est possible que si
ℓ'- ε - (ℓ+ε) ≤0
À partir d'un certain rang, tous les termes de la suite u sont dans cet intervalle
À partir d'un autre rang, tous les termes de la suite u sont dans cet intervalle
ℓ- ε
ℓ
ℓ+ε
ℓ'- ε
ℓ'
ℓ'+ ε

1. on fait ce choix pour que les deux inégalités soient vérifiées.

Exercice 3.3.1.3 Proposer une autre démonstration en raisonnant par l'absurde.

Exemple 3.3.1.4 Montrons que $(u_n) = \left(\frac{1}{n+1}\right)$ converge vers 0, c'est-à-dire que :

$$\forall \varepsilon > 0 \ , \ \exists n_0 \in \mathbb{N} \ , \ \forall n \geqslant n_0 \ , \ |u_n| \leqslant \varepsilon$$

Soit $\varepsilon > 0$. Posons $n_0 = E\left(\frac{1}{\varepsilon}\right)$. Alors $n_0 \in \mathbb{N}$ et pour tout entier $n \geqslant n_0$:

$$n+1 \geqslant n_0 + 1 \geqslant E(\frac{1}{\varepsilon}) + 1 > \frac{1}{\varepsilon} > 0$$

Par suite, $0 \leqslant \frac{1}{n+1} < \varepsilon$ et donc $|u_n - 0| \leqslant \varepsilon$. D'où $\lim\limits_{n\to+\infty} \frac{1}{n} = 0$.

Exemple 3.3.1.5 Montrons que $\lim\limits_{n\to+\infty} \ln(1 + \frac{1}{n+1}) = 0$. Soit $\varepsilon > 0$. On cherche un entier $n_0 \in \mathbb{N}$ tel que :

$$\forall n \geqslant n_0 \ , \ |\ln(1 + \frac{1}{n+1}) - 0| \leqslant \varepsilon$$

Soit $n \in \mathbb{N}$. Pour que l'inégalité précédente soit vérifiée, (il faut et) il suffit que :

$$\ln(1 + \frac{1}{n+1}) \leqslant \varepsilon \text{ c'est-à-dire } \ 1 + \frac{1}{n+1} \leqslant e^{\varepsilon}$$

soit encore $\frac{1}{n+1} \leqslant e^{\varepsilon} - 1$. S'agissant de nombres strictement positifs, (il faut et) il suffit donc que : $n + 1 \geqslant \frac{1}{e^{\varepsilon} - 1}$. On pose alors $n_0 = E\left(\frac{1}{e^{\varepsilon} - 1}\right)$. Alors $n_0 \in \mathbb{N}$ et par construction,

$$\forall n \geqslant n_0 \ , \ |\ln(1 + \frac{1}{n+1}) - 0| \leqslant \varepsilon$$

Ce qui prouve que $\lim\limits_{n\to+\infty} \ln\left(1 + \frac{1}{n+1}\right) = 0$.

Remarques : *dans la définition de la limite, pour $\varepsilon > 0$ fixé, il existe un entier n_0 tel que pour tout $n \geqslant n_0$, $|u_n - \ell| \leqslant \varepsilon$. Il faut noter quatre points :*

- *tout d'abord, on devrait noter $n_0(\varepsilon)$ et non n_0 car l'entier n_0 dépend du choix de ε. Par convention, on ne l'écrit pas (ce qui permet d'alléger les notations) mais c'est une bonne habitude de bien réfléchir à la dépendance de n_0 par rapport à d'autres « variables » ;*
- *l'entier n_0 n'est pas du tout unique ! En effet, si n_0 convient, tout entier $n_1 \geqslant n_0$ convient aussi : $\forall n \geqslant n_1 \ , \ |u_n - \ell| \leqslant \varepsilon$;*

- *dans le raisonnement précédent, remarquez bien qu'on ne cherche pas nécessairement à trouver le "meilleur" n_0 possible, c'est-à-dire le plus petit entier n_0 qui convient. C'est pour cela qu'on cherche une condition suffisante sur n_0 et non une condition nécessaire et suffisante ;*
- *enfin, pour la rédaction, il y a une différence importante entre l'écriture en langage formel mathématique et l'écriture en français :*
  - $\forall \varepsilon > 0$, $\exists n_0 \in \mathbb{N}$, $\forall n \geqslant n_0$, $|u_n - \ell| \leqslant \varepsilon$
  - *Soit $\varepsilon > 0$. Il existe $n_0 \in \mathbb{N}$ tel que : $\forall n \geqslant n_0$, $|u_n - \ell| \leqslant \varepsilon$.*

  Dans le premier cas, ni $\varepsilon > 0$, ni n_0 ne sont "fixés". Dans le second cas, la phrase en toutes lettres "il existe $n_0 \in \mathbb{N}$ tel que" signifie en réalité "il existe et on choisit un $n_0 \in \mathbb{N}$ tel que".

Remarque : *il est parfois très difficile de prouver la convergence en utilisant la définition ! Par exemple pour la suite définie par $u_0 = 1$ et $u_{n+1} = \sin(u_n)$, on verra plus loin que cette suite converge vers 0 mais il est quasi impossible de le prouver directement à partir de la définition de la limite. C'est pour cette raison (mais pas que pour cette raison) qu'on établira plus loin (paragraphe 4) des théorèmes d'existence de limite. Dans la pratique, ce sont ces théorèmes qu'on utilisera pour prouver la convergence et pas la définition.*

Remarque importante : *on a de manière évidente pour $x \in \mathbb{R}$:*

$$\forall \varepsilon > 0 \ , \ |x| \leqslant \varepsilon \iff \exists k > 0 \ , \ \forall \varepsilon > 0 \ , \ |x| \leqslant k \times \varepsilon$$

C'est pour cette raison que souvent, dans les démonstrations de convergence, quand on prouvera par exemple que :

$$\forall \varepsilon > 0 \ , \ \exists n_0 \in \mathbb{N} \ , \ \forall n \geqslant n_0 \ , \ |u_n - \ell| \leqslant 2\varepsilon$$

on dira qu'on a prouvé la convergence.

Exercice 3.3.1.6 Montrer que $\lim\limits_{n \to +\infty} \dfrac{1}{2^n} = 0$.

Exercice 3.3.1.7 Montrer que $\lim\limits_{n \to +\infty} \dfrac{n^2 - n + 1}{n^2 + n + 1} = 1$.

Proposition 3.3.1.8 *Soient $(u_n)_{n \in \mathbb{N}}$ une suite réelle et $\ell \in \mathbb{R}$. Alors (u_n) converge vers ℓ si et seulement si la suite $(u_n - \ell)$ converge vers 0.*

Preuve :

C'est évident !

$\boxtimes$

Proposition 3.3.1.9 *Toute suite convergente est bornée.*

Preuve :

Soit $(u_n)_{n\in\mathbb{N}}$ une suite convergente et soit $\ell = \lim_{n\to+\infty} u_n$.
Soit $\varepsilon = 1 > 0$. Par définition de la limite, il existe un entier n_0 tel que : $\forall n \geqslant n_0$, $|u_n - \ell| \leqslant 1$. On pose alors $m = \max\{|u_n| \ , \ n \in [\![0, n_0]\!]\}$ (ou de façon moins formelle $m = \max\{|u_0|, \cdots, |u_{n_0}|\}$) et $M = \max\{m, |\ell|+1\}$.

Montrons que pour tout entier n, $|u_n| \leqslant M$. Soit $n \in \mathbb{N}$. On distingue deux cas :

- si $n < n_0$, alors par définition de m, $|u_n| \leqslant m \leqslant M$;
- si $n \geqslant n_0$, alors : $|u_n| = |u_n - \ell + \ell| \leqslant |u_n - \ell| + |\ell| \leqslant |\ell| + 1 \leqslant M$.

Ce qui prouve que $(u_n)_{n\in\mathbb{N}}$ est bornée.

⊠

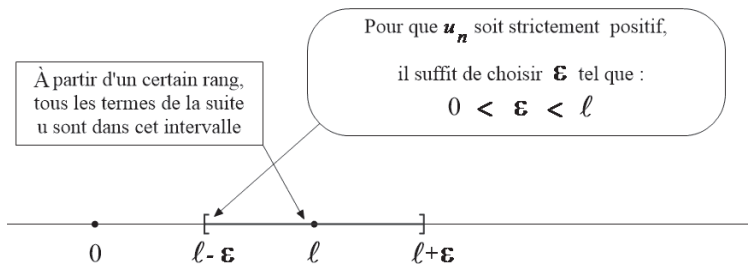
⚠ **Attention :** la réciproque est très fausse ! Une suite bornée n'est pas nécessairement convergente ! On verra plus loin que la suite $((-1)^n)_{n\in\mathbb{N}}$ est une suite bornée qui ne converge pas.

3.3.2 Convergence et signe

Proposition 3.3.2.1 *Si $(u_n)_{n\in\mathbb{N}}$ converge vers $\ell > 0$, alors $(u_n)_{n\in\mathbb{N}}$ est minorée, à partir d'un certain rang, par un réel strictement positif. En particulier, à partir d'un certain rang, tous les termes de la suite sont strictement positifs.*

Preuve :

On peut commencer par étudier la situation sur un dessin :


Pour que u_n soit strictement positif,
il suffit de choisir ε tel que :
$0 < \varepsilon < \ell$
À partir d'un certain rang, tous les termes de la suite u sont dans cet intervalle
0
$\ell - \varepsilon$
ℓ
$\ell + \varepsilon$

Soit $\varepsilon = \frac{\ell}{2} > 0$. La suite $(u_n)_{n\in\mathbb{N}}$ converge vers ℓ donc :

$$\exists n_0 \in \mathbb{N} \ , \ \forall n \geqslant n_0 \ , \ |u_n - \ell| \leqslant \varepsilon$$

On fixe un tel entier n_0. On a alors pour tout entier $n \geqslant n_0$:

$$u_n \geqslant \ell - \varepsilon \geqslant \frac{\ell}{2} > 0$$

Ainsi, à partir du rang n_0, la suite $(u_n)_{n\geqslant n_0}$ est minorée par $\frac{\ell}{2} > 0$.

⊠

Corollaire 3.3.2.2 *Si $(u_n)_{n\in\mathbb{N}}$ converge vers $\ell < 0$, alors $(u_n)_{n\in\mathbb{N}}$ est majorée, à partir d'un certain rang, par un réel strictement négatif. En particulier, à partir d'un certain rang, tous les termes de la suite sont strictement négatifs.*

Preuve :

On applique la proposition précédente à la suite $-(u_n)_{n\in\mathbb{N}}$.

⊠

⚠ **Attention :** ces résultats sont très faux si $\ell = 0$!!! Si $(u_n)_{n\in\mathbb{N}}$ converge vers 0, alors on ne peut pas en déduire que $u_n \geqslant 0$ à partir d'un certain rang ou bien $u_n \leqslant 0$ à partir d'un certain rang. Par exemple, la suite $(\frac{(-1)^n}{n+1})$ converge vers 0 mais n'est jamais de signe constant à partir d'un certain rang.

3.3.3 Divergence d'une suite

Définition 3.3.3.1 On dit qu'une suite est divergente si elle n'est pas convergente, c'est-à-dire si elle vérifie :

$$\forall \ell \in \mathbb{R} \ , \ \exists \varepsilon > 0 \ , \ \forall N \in \mathbb{N} \ , \ \exists n \geqslant N \ , \ |u_n - \ell| > \varepsilon$$

Pour les suites réelles, on va voir qu'en fait, il y a deux modes différents de divergence : soit la suite tend vers l'infini (plus l'infini ou moins l'infini) soit elle n'a tout simplement pas de limite. Il faudra d'ailleurs faire très attention au vocabulaire : une suite converge signifie qu'elle admet une limite finie. Une suite admet une limite signifie que soit elle est convergente, soit elle admet une limite infinie.

3.3.3.a Divergence vers $+\infty$ ou vers $-\infty$

De façon informelle, (u_n) tend vers $+\infty$ signifie que u_n devient aussi grand que l'on veut à partir d'un certain rang. Autrement dit, si on se donne un réel A, à partir d'un certain rang tous les termes de la suite sont plus grands que A. Ceci nous amène à poser les définitions formelles suivantes.

Définition 3.3.3.2 On dit qu'une suite (u_n) admet $+\infty$ pour limite (ou tend vers $+\infty$) si elle vérifie :

$$\forall A \in \mathbb{R} \ , \ \exists N \in \mathbb{N} \ , \ \forall n \geqslant N \ , \ u_n \geqslant A$$

On note alors $\lim\limits_{n\to+\infty} u_n = +\infty$.

On dit qu'une suite $(u_n)_{n\in\mathbb{N}}$ tend vers $-\infty$ (ou qu'elle admet $-\infty$ pour limite) si :

$$\forall A \in \mathbb{R} \ , \ \exists N \in \mathbb{N} \ , \ \forall n \geqslant N \ , \ u_n \leqslant A$$

On note alors $\lim\limits_{n\to+\infty} u_n = -\infty$.

Exercice 3.3.3.3 Interpréter graphiquement ces définitions.

Exemple 3.3.3.4 La suite $(u_n) = (n)$ tend vers $+\infty$. En effet, soit $A \in \mathbb{R}$. En posant $n_0 = \max(E(A)+1, 0)$, $n_0 \in \mathbb{N}$ et pour tout entier $n \geqslant n_0$, $u_n = n \geqslant n_0 \geqslant E(A)+1 \geqslant A$.

Proposition 3.3.3.5 *Une suite qui tend vers $+\infty$ (ou $-\infty$) est une suite divergente. On dit aussi que (u_n) diverge vers $+\infty$ (respectivement vers $-\infty$).*

Preuve :

Traitons le cas d'une suite qui tend vers $+\infty$. On doit montrer que :

$$\forall \ell \in \mathbb{R} \ , \ \exists \varepsilon > 0 \ , \ \forall N \in \mathbb{N} \ , \ \exists n \geqslant N \ , \ |u_n - \ell| > \varepsilon$$

Soit $\ell \in \mathbb{R}$. Posons $\varepsilon = 1 > 0$ et $A = \ell + 2$.
Par définition de $\lim\limits_{n\to+\infty} u_n = +\infty$, il existe un entier n_0 tel que, pour tout entier $n \geqslant n_0$, $u_n \geqslant \ell + 2$.
Alors pour tout entier N, $n = \max(n_0, N) \geqslant N$ et $|u_n - \ell| \geqslant 2 > \varepsilon$. Ce qui montre que $(u_n)_{n\in\mathbb{N}}$ diverge.

⊠

Proposition 3.3.3.6 *Soit $(u_n)_{n\in\mathbb{N}}$ une suite réelle. Alors :*

(i) Si $(u_n)_{n\in\mathbb{N}}$ diverge vers $+\infty$, $(u_n)_{n\in\mathbb{N}}$ est minorée mais n'est pas majorée ;

(ii) Si $(u_n)_{n\in\mathbb{N}}$ diverge vers $-\infty$, $(u_n)_{n\in\mathbb{N}}$ est majorée mais n'est pas minorée.

Enfin, les deux réciproques sont fausses.

Preuve :

• (i) Soit $(u_n)_{n\in\mathbb{N}}$ une suite qui diverge vers $+\infty$. Pour commencer,

$$\begin{aligned}(u_n)_{n\in\mathbb{N}} \text{ n'est pas majorée} &\iff \rceil\,(\exists M\in\mathbb{R}\ ,\ \forall n\in\mathbb{N}\ ,\ u_n\leqslant M)\\ &\iff \forall M\in\mathbb{R}\ ,\ \exists n\in\mathbb{N}\ ,\ u_n>M\end{aligned}$$

Soit $M\in\mathbb{R}$. On applique la définition de la divergence vers $+\infty$ avec « $A=M+1$ » :

$$\exists n_0\in\mathbb{N}\ ,\ \forall n\geqslant n_0\ ,\ u_n\geqslant M+1>M$$

Ce qui prouve que $(u_n)_{n\in\mathbb{N}}$ n'est pas majorée. Par ailleurs, soit un entier n_0 vérifiant la propriété ci-dessus et soient $K=\min\{u_n\ ,\ n\in[\![0,n_0]\!]\}$ et $m=\min\{K,M+1\}$. Il est alors clair que m est un minorant de la suite $(u_n)_{n\in\mathbb{N}}$.

• (ii) se déduit de (i) en considérant la suite $-(u_n)_{n\in\mathbb{N}}$.

• Pour les contre-exemples des réciproques :

∗ la suite définie par : $\forall n\in\mathbb{N}$, $v_n=(1+(-1)^n)n$ est une suite non majorée (puisque $v_{2n}=4n$ pour tout entier n) mais qui ne diverge pas vers $+\infty$ puisque $v_{2n+1}=0$ pour tout $n\in\mathbb{N}$;

∗ on peut prendre $(w_n)_{n\in\mathbb{N}}=-(v_n)_{n\in\mathbb{N}}$ qui donne un exemple de suite non minorée mais qui ne diverge pas vers $-\infty$.

⊠

⚠ **Attention :** retenez bien qu'une suite qui n'est pas majorée ne diverge pas forcément vers $+\infty$! C'est une erreur grave et malheureusement fréquente !

3.3.3.b Autres modes de divergence

Une suite qui diverge ne tend pas forcément vers $+\infty$ ou $-\infty$: elle peut simplement ne pas admettre de limite.

Par exemple, considérons la suite $(u_n)_{n\in\mathbb{N}}$ définie par $u_n = (-1)^n$ pour tout entier n. Montrons que la suite $(u_n)_{n\in\mathbb{N}}$ diverge, c'est-à-dire que :

$$\forall \ell \in \mathbb{R}\ ,\ \exists \varepsilon > 0\ ,\ \forall N \in \mathbb{N}\ ,\ \exists n \geqslant N\ ,\ |u_n - \ell| > \varepsilon$$

Soit $\ell \in \mathbb{R}$. Posons $\varepsilon = \dfrac{1}{2}$ et soit $N \in \mathbb{N}$. Alors, il y a deux possibilités :

- soit $|u_N - \ell| > \varepsilon$ (et dans ce cas, il existe $n = N \geqslant N$ tel que $|u_n - \ell| > \varepsilon$) ;
- ou bien $|u_N - \ell| \leqslant \varepsilon$. Mais dans ce cas, on a :

$$|u_{N+1} - \ell| = |u_{N+1} - u_N + u_N - \ell| \geqslant |u_{N+1} - u_N| - |u_N - \ell| \geqslant 2 - \varepsilon > \varepsilon$$

et dans ce cas, il existe $n = N + 1 \geqslant N$ tel que $|u_n - \ell| > \varepsilon$.

Ce qui prouve que $(u_n)_{n\in\mathbb{N}}$ diverge.

Remarque : *on reverra un peu plus loin une méthode beaucoup plus simple pour prouver la divergence de cette suite, utilisant les suites extraites.*

3.3.4 Opérations sur les suites convergentes

3.3.4.a Espace vectoriel des suites convergeant vers 0

Proposition 3.3.4.1 *L'ensemble $\mathcal{S}_0$ des suites qui convergent vers 0 est un espace vectoriel : c'est un sous-espace vectoriel de l'ensemble des suites réelles. Autrement dit, $\mathcal{S}_0$ n'est pas vide et est stable par combinaisons linéaires :*

$$\forall (u_n)_{n\in\mathbb{N}}, (v_n)_{n\in\mathbb{N}} \in \mathcal{S}_0\ ,\ \forall \lambda, \mu \in \mathbb{R}\ ,\ \lambda(u_n)_{n\in\mathbb{N}} + \mu(v_n)_{n\in\mathbb{N}} \in \mathcal{S}_0$$

Preuve :

Montrons que $(\mathcal{S}_0, +, \cdot)$ est un sous espace vectoriel de $(\mathbb{R}^{\mathbb{N}}, +, \cdot)$.

- $\mathcal{S}_0$ est non vide car il contient la suite nulle qui converge bien vers 0.
- Montrons que $\mathcal{S}_0$ est stable par combinaisons linéaires. Soient $u = (u_n)_{n\in\mathbb{N}}$ et $v = (v_n)_{n\in\mathbb{N}}$ deux suites qui convergent vers 0, et soit $\lambda \in \mathbb{R}$. Montrons que :

  (i) $(u + v)$ converge vers 0 ;

  (ii) $(\lambda \cdot u)$ converge vers 0.

  Ceci nous permettra de conclure, d'après (ii), que si $(\lambda, \mu) \in \mathbb{R}^2$, alors $\lambda \cdot u$ et $\mu \cdot v$ convergent vers 0 et donc d'après (i), la somme, $\lambda \cdot u + \mu \cdot v$ converge vers 0.

(*i*) Convergence de $u + v$ vers 0.
Soit $\varepsilon > 0$. Alors :

$$\exists n_1 \in \mathbb{N} \ , \ \forall n \geqslant n_1 \ , \ |u_n| \leqslant \frac{\varepsilon}{2} \quad \text{(convergence de } u \text{ vers 0)}$$

$$\exists n_2 \in \mathbb{N} \ , \ \forall n \geqslant n_2 \ , \ |v_n| \leqslant \frac{\varepsilon}{2} \quad \text{(convergence de } v \text{ vers 0)}$$

Soient n_1 et n_2 deux tels entiers. Alors, pour tout entier naturel $n \geqslant \max(n_1, n_2)$, $|u_n + v_n| \leqslant |u_n| + |v_n| \leqslant \varepsilon$.
D'où le résultat, c'est-à-dire $(u + v) \in \mathcal{S}_0$.

(*ii*) Convergence de $\lambda \cdot u$.
Si $\lambda = 0$, alors $\lambda \cdot u = 0$ (suite nulle) et donc $\lambda \cdot u$ converge vers 0. On suppose à présent que $\lambda \neq 0$. Soit $\varepsilon > 0$. Par définition de la convergence, il existe un entier $n_1 \in \mathbb{N}$ tel que :

$$\forall n \geqslant n_1 \ , \ |u_n| \leqslant \frac{\varepsilon}{|\lambda|} \quad \text{(convergence de } u \text{ vers 0)}$$

Alors, pour tout $n \geqslant n_1$, $|\lambda u_n| = |\lambda| \times |u_n| \leqslant \varepsilon$, prouvant ainsi que $\lambda \cdot u$ converge également vers 0.

⊠

Remarque : *en fait, on a montré que toute suite convergente est bornée. On aurait donc également pu montrer que $\mathcal{S}_0$ est un sous-espace vectoriel de $\mathcal{B}(\mathbb{N}, \mathbb{R})$.*

Proposition 3.3.4.2 *Si $(u_n)_{n\in\mathbb{N}}$ converge vers 0 et si $(v_n)_{n\in\mathbb{N}}$ est bornée, alors $(u_n v_n)$ converge vers 0.*

Preuve :

Par hypothèse, la suite $(v_n)_{n\in\mathbb{N}}$ est bornée. Soit $M \in \mathbb{R}^+$ tel que :

$$\forall n \in \mathbb{N} \ , \ |v_n| \leqslant M$$

Soit $\varepsilon > 0$. $(u_n)_{n\in\mathbb{N}}$ converge vers 0 donc il existe $n_0 \in \mathbb{N}$ tel que :

$$\forall n \geqslant n_0 \ , \ |u_n| \leqslant \frac{\varepsilon}{M+1}$$

Alors,

$$\forall n \geqslant n_0 \ , \ |u_n v_n| = |u_n| \times |v_n| \leqslant M \times \frac{\varepsilon}{M+1} \leqslant \varepsilon$$

Ce qui prouve que la suite $(u_n v_n)_{n\in\mathbb{N}}$ converge vers 0.

⊠

Exemple 3.3.4.3 Soit $(u_n)_{n\geqslant 1}$ définie par : $\forall n \geqslant 1$, $u_n = \dfrac{\sin(n)}{n}$.
On a pour tout entier $n \geqslant 1$, $u_n = \dfrac{1}{n} \times \sin(n)$. Or, $(\frac{1}{n})_{n\geqslant 1}$ converge vers 0 et $(\sin(n))_{n\geqslant 1}$ est bornée. Par conséquent, $(u_n)_{n\geqslant 1}$ converge vers 0.

Remarque : *notez qu'ici la suite* $(\sin(n))_{n\in\mathbb{N}}$ *n'admet pas de limite (voir les exercices pour une preuve rigoureuse) donc on ne peut pas appliquer les règles sur les produits de limite (voir paragraphe suivant).*

3.3.4.b Opérations algébriques sur les limites

Proposition 3.3.4.4 *L'ensemble des suites convergentes est un sous-anneau de l'ensemble des suites bornées et un sous-espace vectoriel. De plus, on a les règles suivantes :*

Limite d'une somme

$\lim\limits_{n\to+\infty} u_n$	ℓ	ℓ *ou* $+\infty$	ℓ *ou* $-\infty$	$+\infty$
$\lim\limits_{n\to+\infty} v_n$	ℓ'	$+\infty$	$-\infty$	$-\infty$
$\lim\limits_{n\to+\infty} (u_n+v_n)$	$\ell+\ell'$	$+\infty$	$-\infty$	*? ? ?*

Limite d'un produit

$\lim\limits_{n\to+\infty} u_n$	ℓ	$\ell>0$ *ou* $+\infty$	$\ell<0$ *ou* $-\infty$	$\ell>0$ *ou* $+\infty$	$\ell<0$ *ou* $-\infty$	0
$\lim\limits_{n\to+\infty} v_n$	ℓ'	$+\infty$	$+\infty$	$-\infty$	$-\infty$	$\pm\infty$
$\lim\limits_{n\to+\infty} (u_n v_n)$	$\ell\times\ell'$	$+\infty$	$-\infty$	$-\infty$	$+\infty$	*? ? ?*

Et enfin :

Limite de l'inverse d'une suite

$\lim\limits_{n\to+\infty} u_n$	$\ell \neq 0$	$\ell = 0$ et $u_n > 0$	$\ell = 0$ et $u_n < 0$	$\pm\infty$
$\lim\limits_{n\to+\infty} \dfrac{1}{u_n}$	$\dfrac{1}{\ell}$	$+\infty$	$-\infty$	0

Limite d'un quotient

$\lim\limits_{n\to+\infty} u_n$	ℓ	ℓ	$+\infty$	$+\infty$	$-\infty$	$-\infty$
$\lim\limits_{n\to+\infty} v_n$	$\ell' \neq 0$	$\pm\infty$	$\ell' > 0$	$\ell' < 0$	$\ell' > 0$	$\ell' < 0$
$\lim\limits_{n\to+\infty} \dfrac{u_n}{v_n}$	$\dfrac{\ell}{\ell'}$	0	$+\infty$	$-\infty$	$-\infty$	$+\infty$

et

$\lim\limits_{n\to+\infty} u_n$	$\pm\infty$	$\ell > 0$ ou $+\infty$	$\ell > 0$ ou $+\infty$	$\ell < 0$ ou $-\infty$	$\ell < 0$ ou $-\infty$	0
$\lim\limits_{n\to+\infty} v_n$	$\pm\infty$	0^+	0^-	0^+	0^-	0
$\lim\limits_{n\to+\infty} \dfrac{u_n}{v_n}$	???	$+\infty$	$-\infty$	$-\infty$	$+\infty$	???

Dans ces tableaux, la notation ??? signifie qu'il s'agit d'une forme indéterminée, c'est-à-dire qu'on ne peut pas conclure directement que la suite a (ou non) une limite.

Preuve :

• Montrons pour commencer que si $(u_n)_{n\in\mathbb{N}}$ converge vers ℓ et $(v_n)_{n\in\mathbb{N}}$ converge vers ℓ', où $\ell, \ell' \in \mathbb{R}$, alors $(u_n)_{n\in\mathbb{N}} + (v_n)_{n\in\mathbb{N}}$ converge vers $\ell + \ell'$.

Soient $(u'_n) = (u_n - \ell)$ et $(v'_n) = (v_n - \ell')$. Par hypothèse, $(u'_n)_{n\in\mathbb{N}}$ et $(v'_n)_{n\in\mathbb{N}}$ convergent vers 0. Or, on a montré que $\mathcal{S}_0$, l'ensemble des suites qui convergent vers 0, est un espace vectoriel. Par suite, $(u'_n)_{n\in\mathbb{N}} + (v'_n)_{n\in\mathbb{N}}$ converge vers 0, ce qui équivaut à dire que $(u_n)_{n\in\mathbb{N}} + (v_n)_{n\in\mathbb{N}}$ converge vers $\ell + \ell'$.

• Montrons que si $(u_n)_{n\in\mathbb{N}}$ diverge vers $+\infty$ et $(v_n)_{n\in\mathbb{N}}$ converge vers ℓ', alors $(u_n)_{n\in\mathbb{N}} + (v_n)_{n\in\mathbb{N}}$ diverge vers $+\infty$.
Pour commencer, $(v_n)_{n\in\mathbb{N}}$ converge : par conséquent, $(v_n)_{n\in\mathbb{N}}$ est bornée. Soit $M \in \mathbb{R}^+$ tel que $|v| \leqslant M$ (relation entre suites). Par ailleurs, soit $A \in \mathbb{R}$. La suite $(u_n)_{n\in\mathbb{N}}$ diverge vers $+\infty$ donc :

$$\exists n_0 \in \mathbb{N} \ , \ \forall n \geqslant n_0 \ , \ u_n \geqslant A + M$$

On fixe un tel entier n_0. On a alors :

$$\forall n \geqslant n_0 \ , \ u_n + v_n \geqslant A + M - M \geqslant A$$

Ce qui prouve que $(u_n)_{n\in\mathbb{N}} + (v_n)_{n\in\mathbb{N}}$ diverge vers $+\infty$.

• Montrons à présent que si $(u_n)_{n\in\mathbb{N}}$ converge vers $\ell \in \mathbb{R}$ et $(v_n)_{n\in\mathbb{N}}$ converge vers $\ell' \in \mathbb{R}$, alors $(u_n v_n)_{n\in\mathbb{N}}$ converge vers $\ell\ell'$. Pour cela, on remarque que :

$$\forall n \in \mathbb{N} \ , \ u_n v_n - \ell\ell' = u_n v_n - u_n \ell' + u_n \ell' - \ell\ell' = u_n(v_n - \ell') + \ell'(u_n - \ell)$$

Par hypothèse, $(v_n - \ell')_{n\in\mathbb{N}}$ converge vers 0 et puisque $(u_n)_{n\in\mathbb{N}}$ converge, $(u_n)_{n\in\mathbb{N}}$ est bornée. Ainsi, $(u_n)_{n\in\mathbb{N}} \times (v_n - \ell')_{n\in\mathbb{N}}$ est le produit d'une suite bornée et d'une suite qui converge vers 0 : d'après la dernière proposition, cette suite converge vers 0.
De même, $\ell'(u_n - \ell)_{n\in\mathbb{N}}$ converge vers 0. $\mathcal{S}_0$ étant un espace vectoriel, $(u_n v_n - \ell\ell')_{n\in\mathbb{N}} \in \mathcal{S}_0$, c'est-à-dire $(u_n v_n)_{n\in\mathbb{N}}$ converge vers $\ell\ell'$.

• Montrons que si $(u_n)_{n\in\mathbb{N}}$ diverge vers $-\infty$ et $(v_n)_{n\in\mathbb{N}}$ converge vers $\ell' < 0$, alors $(u_n v_n)_{n\in\mathbb{N}}$ diverge vers $+\infty$.
Tout d'abord, $(v_n)_{n\in\mathbb{N}}$ converge vers $\ell' < 0$: on a vu que dans ce cas, la suite $(v_n)_{n\in\mathbb{N}}$ est majorée à partir d'un certain rang par un réel strictement négatif, c'est-à-dire :

$$\exists n_0 \in \mathbb{N} \ , \ \exists M < 0 \ , \ \forall n \geqslant n_0 \ , \ v_n \leqslant M$$

On fixe un tel entier n_0 et un tel réel $M < 0$. Soit $A > 0$. La suite $(u_n)_{n\in\mathbb{N}}$ diverge vers $-\infty$: il existe un entier n_1 tel que, $\forall n \geqslant n_1$, $u_n \leqslant \frac{A}{M} < 0$. On a alors :

$$\forall n \geqslant \max(n_0, n_1) \ , \ u_n v_n \geqslant A$$

Ce qui prouve que $(u_n v_n)$ diverge vers $+\infty$.

• Montrons enfin que si $(u_n)_{n\in\mathbb{N}}$ converge vers $\ell \neq 0$, alors $(\frac{1}{u_n})_{n\in\mathbb{N}}$ converge vers $\frac{1}{\ell}$.

Quitte à travailler avec $(-u_n)$, on peut supposer que $\ell > 0$. La suite $(u_n)_{n\in\mathbb{N}}$ converge vers $\ell > 0$: il existe un entier n_0 et un réel $M > 0$ tels que $(u_n)_{n\geqslant n_0}$ est minorée par M. On remarque alors que :

$$\forall n \geqslant n_0 \ , \ \frac{1}{u_n} - \frac{1}{\ell} = \frac{1}{u_n \ell} \times (\ell - u_n)$$

Or, pour tout entier $n \geqslant n_0$, $0 \leqslant \frac{1}{\ell u_n} \leqslant \frac{1}{\ell M}$, c'est-à-dire que la suite $(\frac{1}{\ell u_n})_{n\geqslant n_0}$ est bornée. De plus, $(\ell - u_n)_{n\geqslant n_0}$ converge vers 0. Par conséquent, leur produit converge vers 0, *i.e.* $(\frac{1}{u_n})_{n\geqslant n_0}$ converge vers $\frac{1}{\ell}$.

⊠

Remarque : *la majeure partie des autres résultats de la proposition se déduisent des propriétés qu'on a démontré (en remplaçant u par $-u$ et/ou v par $-v$ et en remarquant que le quotient est le produit d'une suite et de l'inverse de l'autre).*

Exercice 3.3.4.5 En fait, toutes les propriétés ne se déduisent pas de celles qu'on a prouvées ! Lesquelles reste-t-il à prouver ? Prouver ces propriétés.

Exercice 3.3.4.6 Déterminer les limites des suites suivantes :

$$u_n = \frac{n^2 + 3n - 1}{n^2 - 3n + 1732} \quad ; \quad v_n = \sqrt{n+1} - \sqrt{n}$$

$$w_n = \frac{\ln n}{n^\alpha} \text{ où } \alpha \in \mathbb{R} \text{ est fixé} \quad ; \quad z_n = 2^{n^2} - \pi^{3n}$$

$$a_n = \frac{\cos(n)}{n} + e^n \sin(e^{-n}) \quad ; \quad b_n = n^2 \ln(\cos(\frac{1}{n}))$$

On pourra utiliser les équivalents des fonctions usuelles pour faire apparaître des limites que l'on sait calculer.

3.3.5 Compatibilité du passage à la limite avec la relation d'ordre

Proposition 3.3.5.1 *Soient $(u_n)_{n\in\mathbb{N}}$ et $(v_n)_{n\in\mathbb{N}}$ deux suites réelles telles que, à partir d'un certain rang $n_0 \in \mathbb{N}$, $u_n \leqslant v_n$ (pour $n \geqslant n_0$).*

(i) Si $\lim\limits_{n\to+\infty} u_n$ et $\lim\limits_{n\to+\infty} v_n$ existent dans $\overline{\mathbb{R}}$, alors $\lim\limits_{n\to+\infty} u_n \leqslant \lim\limits_{n\to+\infty} v_n$ (on dit que les inégalités au sens large passent à la limite).

(ii) Si $\lim\limits_{n\to+\infty} u_n = +\infty$, alors $\lim\limits_{n\to+\infty} v_n = +\infty$.

(iii) Si $\lim\limits_{n\to+\infty} v_n = -\infty$, alors $\lim\limits_{n\to+\infty} u_n = -\infty$.

Preuve :

• On commence par (ii).
On suppose que $\lim\limits_{n\to+\infty} u_n = +\infty$ et on montre que $\lim\limits_{n\to+\infty} v_n = +\infty$.
Soit $A \in \mathbb{R}$. Par définition de la divergence vers $+\infty$:

$$\exists n_1 \in \mathbb{N} \ , \forall n \geqslant n_1 \ , \ u_n \geqslant A$$

Soit un tel entier n_1. Par ailleurs, par hypothèse, $\forall n \geqslant n_0 \ , \ u_n \leqslant v_n$.
Posons $N = \max(n_0, n_1)$. On a alors :

$$\forall n \geqslant N \ , \ v_n \geqslant u_n \geqslant A$$

D'où (ii).

• (iii) s'obtient en appliquant (ii) aux suites $(-v_n)$ et $(-u_n)$.

• Enfin, montrons (i). Pour commencer, on remarque que :

∗ si $\lim\limits_{n\to+\infty} u_n = -\infty$ ou si $\lim\limits_{n\to+\infty} v_n = +\infty$, il n'y a rien à prouver ;

∗ si $\lim\limits_{n\to+\infty} u_n = +\infty$ ou $\lim\limits_{n\to+\infty} v_n = -\infty$, on applique (ii) ou (iii).

Il reste donc le cas où $\lim\limits_{n\to+\infty} u_n = \ell \in \mathbb{R}$ et $\lim\limits_{n\to+\infty} v_n = \ell' \in \mathbb{R}$.

Soit $\varepsilon > 0$. La suite $(u_n)_{n\in\mathbb{N}}$ converge vers ℓ donc :

$$\exists n_1 \in \mathbb{N} \ , \forall n \geqslant n_1 \ , \ \ell - \varepsilon \leqslant u_n \leqslant \ell + \varepsilon$$

Soit un tel entier n_1. De même, il existe un entier n_2 tel que :

$$\forall n \geqslant n_2 \ , \ \ell' - \varepsilon \leqslant v_n \leqslant \ell' + \varepsilon$$

Par ailleurs, par hypothèse, $\forall n \geqslant n_0$, $u_n \leqslant v_n$. Soit $n = \max(n_0, n_1, n_2)$. On a alors :

$$\ell - \varepsilon \leqslant u_n \leqslant v_n \leqslant \ell' + \varepsilon \quad \text{par suite} \quad \ell \leqslant \ell' + 2\varepsilon$$

Ainsi, on a montré que : $\forall \varepsilon > 0$, $\ell \leqslant \ell' + 2\varepsilon$. Par conséquent, $\ell \leqslant \ell'$.

⊠

Exemple 3.3.5.2 On considère la suite définie par : $\forall n \in \mathbb{N}$, $u_n = n + \sin(n)$. Pour tout entier $n \in \mathbb{N}$, $u_n \geqslant n - 1$ et $\lim\limits_{n\to+\infty} (n-1) = +\infty$. Par conséquent, $\lim\limits_{n\to+\infty} u_n = +\infty$.

Remarque : *dans l'exemple précédent, on pouvait aussi simplement factoriser par n et montrer que* $(u_n) = (n) \times (v_n)$ *avec* $\lim\limits_{n\to+\infty} v_n = 1$. *On conclut alors en utilisant les opérations algébriques sur les limites.*

⚠ **Attention :** le passage à la limite conserve les inégalités larges, mais pas les inégalités strictes !

$$\begin{cases} (u_n) \text{ et } (v_n) \text{ convergent} \\ \forall n \in \mathbb{N} \text{ , } u_n < v_n \end{cases} \not\Longrightarrow \lim_{n\to+\infty} u_n < \lim_{n\to+\infty} v_n$$

En particulier, voici une erreur grave (et classique) qu'il faut absolument éviter :

$$\begin{cases} (u_n)_{n\in\mathbb{N}} \text{ converge vers } \ell \\ \forall n \in \mathbb{N} \text{ , } 0 < u_n < 1 \end{cases} \not\Longrightarrow 0 < \ell < 1$$

Exercice 3.3.5.3 Donner un exemple très simple de suite $(u_n)_{n\in\mathbb{N}}$ qui converge vers $\ell = 0$ avec $\forall n \in \mathbb{N}$, $u_n > 0$.

Corollaire 3.3.5.4 *Soient* $(u_n)_{n\in\mathbb{N}}$ *et* $(v_n)_{n\in\mathbb{N}}$ *deux suites. Si* $\lim\limits_{n\to+\infty} u_n = +\infty$ *et si* $(v_n)_{n\in\mathbb{N}}$ *est minorée, alors* $\lim\limits_{n\to+\infty} (u_n + v_n) = +\infty$.

Preuve :

C'est une conséquence immédiate du théorème précédent. En effet, si $m \in \mathbb{R}$ est un minorant de la suite $(v_n)_{n\in\mathbb{N}}$, alors pour tout entier n, $u_n + v_n \geqslant u_n + m$. Et d'après les opérations algébriques sur les limites, $\lim\limits_{n\to+\infty} (u_n + m) = +\infty$.

⊠

Théorème 3.3.5.5 (Théorème des gendarmes) *Soient (u_n), (v_n) et (w_n) trois suites réelles. On suppose que :*

(i) il existe $n_0 \in \mathbb{N}$ tel que : $\forall n \geqslant n_0$, $u_n \leqslant v_n \leqslant w_n$;

(ii) $(u_n)_{n\in\mathbb{N}}$ et $(w_n)_{n\in\mathbb{N}}$ convergent vers la même limite ℓ.

Alors $(v_n)_{n\in\mathbb{N}}$ converge et $\lim\limits_{n\to+\infty} v_n = \lim\limits_{n\to+\infty} u_n = \lim\limits_{n\to+\infty} w_n = \ell$.

Preuve :

On écrit les définitions formelles de la limite. Soit $\varepsilon > 0$. Puisque $(u_n)_{n\in\mathbb{N}}$ et $(w_n)_{n\in\mathbb{N}}$ convergent vers ℓ, il existe deux entiers n_1 et n_2 tels que :

$$\forall n \geqslant n_1 \ , \ |u_n - \ell| \leqslant \varepsilon \ \text{ et } \ \forall n \geqslant n_2 \ , \ |w_n - \ell| \leqslant \varepsilon$$

Posons alors $N = \max(n_0, n_1, n_2)$. Alors pour tout entier $n \geqslant N$, on a :

$$\ell - \varepsilon \leqslant u_n \leqslant v_n \leqslant w_n \leqslant \ell + \varepsilon$$

et par conséquent, $|v_n - \ell| \leqslant \varepsilon$. Ce qui prouve que $(v_n)_{n\in\mathbb{N}}$ converge et $\lim\limits_{n\to+\infty} v_n = \ell$.

⊠

Exercice 3.3.5.6 Un étudiant propose la démonstration suivante, beaucoup plus simple :

« *Puisque $u_n \leqslant v_n \leqslant w_n$ et le passage à la limite est compatible avec la relation d'ordre, $\lim\limits_{n\to+\infty} u_n \leqslant \lim\limits_{n\to+\infty} v_n \leqslant \lim\limits_{n\to+\infty} w_n$. Or, $\lim\limits_{n\to+\infty} u_n = \lim\limits_{n\to+\infty} w_n = \ell$ donc $\lim\limits_{n\to+\infty} v_n = \ell$, c'est-à-dire $(v_n)_{n\in\mathbb{N}}$ converge et sa limite est ℓ* ».

Quelle est l'erreur dans ce raisonnement ?

Exemple 3.3.5.7 On considère la suite (v_n) définie par : $\forall n \in \mathbb{N}^\star$, $v_n = \dfrac{E(\ln(n))}{\ln(2n+1)}$.

On souhaite montrer que (v_n) converge et déterminer sa limite.

Ici, le terme qui pose « problème » est le terme en partie entière (que l'on ne peut calculer explicitement). On va donc donner un encadrement de la suite (v_n). D'après les propriétés de la partie entière,

$$\forall n \in \mathbb{N}^\star \ , \ \ln(n) - 1 \leqslant E(\ln(n)) \leqslant \ln(n)$$

Par conséquent, pour tout entier $n \geqslant 1$,

$$\frac{\ln(n) - 1}{\ln(2n+1)} \leqslant v_n \leqslant \frac{\ln(n)}{\ln(2n+1)}$$

Or, pour $n \in \mathbb{N}$ et $n \geqslant 2$,

$$\frac{\ln(2n+1)}{\ln(n)} = \frac{\ln(n) + \ln(2+\frac{1}{n})}{\ln(n)} = 1 + \frac{\ln(2+\frac{1}{n})}{\ln(n)}$$

Il s'ensuit que $\lim\limits_{n\to+\infty} \dfrac{\ln(2n+1)}{\ln(n)} = 1$ (opérations algébriques sur les limites) et donc $\lim\limits_{n\to+\infty} \dfrac{\ln(n)}{\ln(2n+1)} = 1$. De même, $\lim\limits_{n\to+\infty} \dfrac{\ln(n)-1}{\ln(2n+1)} = 1$.

D'après le théorème des gendarmes, la suite (v_n) converge et $\lim\limits_{n\to+\infty} v_n = 1$.

Le théorème des gendarmes est particulièrement efficace lorsqu'on ne peut pas déterminer une expression explicite de v_n en fonction de n mais qu'on sait encadrer v_n par des termes du même ordre de grandeur [2].

Exemple 3.3.5.8 On considère la suite (v_n) définie pour tout entier $n \geqslant 1$ par :

$$v_n = \int_{2n\pi}^{2n\pi+\frac{\pi}{4}} \frac{x\ln(x)}{\cos^2(x)}\,\mathrm{d}x$$

Pour commencer, on peut noter que la suite (v_n) est bien définie car $x \longmapsto \dfrac{x\ln(x)}{\cos^2(x)}$ est continue sur le segment $[2n\pi, 2n\pi+\frac{\pi}{4}]$ pour $n \in \mathbb{N}^\star$.

Dans cet exemple, on ne connaît pas de primitive de cette fonction et on ne peut donc pas calculer explicitement la valeur de cette intégrale. En revanche, pour $n \in \mathbb{N}^\star$, on a :

$$\forall x \in [2n\pi, 2n\pi+\frac{\pi}{4}]\ ,\ \frac{2n\pi\ln(2n\pi)}{\cos^2(x)} \leqslant \frac{x\ln(x)}{\cos^2(x)} \leqslant \frac{(2n\pi+\frac{\pi}{4})\ln(2n\pi+\frac{\pi}{4})}{\cos^2(x)}$$

D'après les propriétés de l'intégrale, on a donc :

$$\int_{2n\pi}^{2n\pi+\frac{\pi}{4}} \frac{2n\pi\ln(2n\pi)}{\cos^2(x)}\,\mathrm{d}x \leqslant \int_{2n\pi}^{2n\pi+\frac{\pi}{4}} \frac{x\ln(x)}{\cos^2(x)}\,\mathrm{d}x \leqslant \int_{2n\pi}^{2n\pi+\frac{\pi}{4}} \frac{(2n\pi+\frac{\pi}{4})\ln(2n\pi+\frac{\pi}{4})}{\cos^2(x)}\,\mathrm{d}x$$

soit encore :

$$2n\pi\ln(2n\pi)\Big[\tan(x)\Big]_{2n\pi}^{2n\pi+\frac{\pi}{4}} \leqslant v_n \leqslant (2n\pi+\frac{\pi}{4})\ln(2n\pi+\frac{\pi}{4})\Big[\tan(x)\Big]_{2n\pi}^{2n\pi+\frac{\pi}{4}}$$

c'est-à-dire

$$2n\pi\ln(2n\pi) \leqslant v_n \leqslant (2n\pi+\frac{\pi}{4})\ln(2n\pi+\frac{\pi}{4})$$

2. voir paragraphe 5 : relations de comparaison pour les suites.

On en déduit alors que pour tout entier $n \geqslant 2$,

$$2n\pi\ln(n)\left(1+\frac{\ln(2\pi)}{\ln(n)}\right) \leqslant v_n \leqslant 2n\pi\ln(n)\left(1+\frac{1}{8n}\right)\left(1+\frac{\ln(2\pi+\frac{\pi}{4n})}{\ln(n)}\right)$$

Or, le calcul direct montre que :

$$\lim_{n\to+\infty} 1+\frac{\ln(2\pi)}{\ln(n)} = 1$$

et par continuité[3] de ln au point 2π,

$$\lim_{n\to+\infty} \left(1+\frac{1}{8n}\right)\left(1+\frac{\ln(2\pi+\frac{\pi}{4n})}{\ln(n)}\right) = 1$$

D'après le théorème des gendarmes, la suite $\left(\dfrac{v_n}{2n\pi\ln(n)}\right)$ converge et sa limite vaut 1.

Ainsi, on a prouvé que $\lim\limits_{n\to+\infty} \dfrac{v_n}{2n\pi\ln(n)} = 1$ (c'est-à-dire $v_n \underset{n\to+\infty}{\sim} 2n\pi\ln(n)$, mais la notion d'équivalent pour les suites n'a pas encore été abordée).

Remarque : *le théorème des gendarmes sera beaucoup utilisé dans les problèmes de recherche d'équivalents. On le reverra dans ce chapitre pour les suites définies implicitement, pour les sommes partielles d'une série à termes positifs divergente et aussi dans le cours de mathématiques spéciales, pour les recherches d'équivalents de série de fonctions ou d'intégrales à paramètre.*

Corollaire 3.3.5.9 *Si $|u_n - \ell| \leqslant \alpha_n$ à partir d'un certain rang avec $\lim\limits_{n\to+\infty} \alpha_n = 0$, alors $(u_n)_{n\in\mathbb{N}}$ converge vers ℓ.*

Preuve :

Soit $n \in \mathbb{N}$. $|u_n - \ell| \leqslant \alpha_n$ équivaut à $-\alpha_n \leqslant u_n - \ell \leqslant \alpha_n$ puis on applique le théorème des gendarmes. ⊠

Exercice 3.3.5.10 Proposer une démonstration directe de ce corollaire, sans utiliser le théorème des gendarmes.

Exercice 3.3.5.11 Quel autre théorème ou propriété ce corollaire permet-il de retrouver directement ?

Exercice 3.3.5.12 Déterminer la limite de la suite $u_n = \dfrac{\ln(n)+5\cos(n)}{n}$.

3. voir le chapitre 6, paragraphe 6.2.5 : caractérisation séquentielle de la continuité.

3.3.6 Convergence et suites extraites

Commençons ce paragraphe par un lemme technique mais utile pour la suite.

Lemme 3.3.6.1 *Soit $\varphi : \mathbb{N} \longrightarrow \mathbb{N}$ strictement croissante. Alors : $\forall n \in \mathbb{N}$, $\varphi(n) \geqslant n$.*

Preuve :

On montre le résultat par récurrence sur n.

Initialisation :
Par définition, $\varphi(0) \in \mathbb{N}$ donc $\varphi(0) \geqslant 0$: la propriété est vraie au rang 0.

Hérédité :

On suppose que la propriété est vraie au rang $n \in \mathbb{N}$: montrons qu'elle est vraie au rang $n+1$. $n+1 > n$ et φ est strictement croissante : par conséquent, $\varphi(n+1) > \varphi(n) \geqslant n$ (d'après l'hypothèse de récurrence). Ainsi, $\varphi(n+1) > n$ et $\varphi(n+1) \in \mathbb{N}$: il s'ensuit que $\varphi(n+1) \geqslant n+1$. Ce qui montre que la propriété est vraie au rang $n+1$ et achève la récurrence.

⊠

Proposition 3.3.6.2 *Soit $(u_n)_{n\in\mathbb{N}}$ une suite qui converge vers $\ell \in \mathbb{R}$. Alors toute suite extraite de $(u_n)_{n\in\mathbb{N}}$ converge aussi vers ℓ.*

Preuve :

Soit $(v_n)_{n\in\mathbb{N}}$ une suite extraite de $(u_n)_{n\in\mathbb{N}}$. Par définition, il existe une application $\varphi : \mathbb{N} \longrightarrow \mathbb{N}$ strictement croissante telle que :

$$\forall n \in \mathbb{N} \ , \ v_n = u_{\varphi(n)}$$

Montrons que $(v_n)_{n\in\mathbb{N}}$ converge vers ℓ. Soit $\varepsilon > 0$. On sait que $(u_n)_{n\in\mathbb{N}}$ converge vers ℓ. Il existe donc un entier n_0 tel que :

$$\forall n \geqslant n_0 \ , \ |u_n - \ell| \leqslant \varepsilon$$

D'après le lemme précédent, si $n \geqslant n_0$, alors $\varphi(n) \geqslant n \geqslant n_0$ et donc :

$$\forall n \geqslant n_0 \ , \ |u_{\varphi(n)} - \ell| \leqslant \varepsilon$$

Ce qui prouve que la suite $(v_n)_{n\in\mathbb{N}}$ converge aussi vers ℓ.

⊠

Remarque : *la proposition précédente se généralise aux suites qui admettent une limite dans $\overline{\mathbb{R}}$ (c'est-à-dire une limite finie ou infinie).*

Exercice 3.3.6.3 Prouver la remarque ! Autrement dit, montrer que si $\lim\limits_{n\to+\infty} u_n = +\infty$, alors toute suite extraite de $(u_n)_{n\in\mathbb{N}}$ diverge vers $+\infty$.

Corollaire 3.3.6.4 *Soit $(u_n)_{n\in\mathbb{N}}$ une suite réelle. S'il existe deux suites extraites de $(u_n)_{n\in\mathbb{N}}$ qui admettent des limites différentes, alors la suite $(u_n)_{n\in\mathbb{N}}$ diverge (et n'admet pas de limite).*

Preuve :

On suppose qu'il existe deux applications φ et ψ strictement croissantes de $\mathbb{N}$ dans $\mathbb{N}$ telles que $(u_{\varphi(n)})$ et $(u_{\psi(n)})$ admettent des limites ℓ_1 et ℓ_2 respectivement, avec $\ell_1 \neq \ell_2$ (et ℓ_1 et ℓ_2 sont dans $\overline{\mathbb{R}}$). Montrons que $(u_n)_{n\in\mathbb{N}}$ n'a pas de limite en raisonnant par l'absurde. Si $(u_n)_{n\in\mathbb{N}}$ admet une limite ℓ (finie ou infinie), alors d'après la proposition précédente (et la remarque), $(u_{\varphi(n)})$ et $(u_{\psi(n)})$ admettent également ℓ pour limite. Par unicité de la limite, $\ell_1 = \ell = \ell_2$, ce qui est absurde.

⊠

▶ Méthode :

Pour prouver la divergence d'une suite $(u_n)_{n\in\mathbb{N}}$, il suffit :

— de prouver que $(u_n)_{n\in\mathbb{N}}$ n'est pas bornée ou qu'il existe une suite extraite non bornée ;

— ou d'exhiber, c'est-à-dire de donner, deux suites extraites de $(u_n)_{n\in\mathbb{N}}$ qui convergent vers des limites différentes.

Exemple 3.3.6.5 Reprenons l'exemple de la suite donnée par $u_n = (-1)^n$ pour tout entier n. La suite extraite (u_{2n}) converge vers 1 (c'est la suite constante égale à 1) et la suite extraite (u_{2n+1}) converge vers -1. Par conséquent, il existe deux suites extraites de $(u_n)_{n\in\mathbb{N}}$ qui ont des limites distinctes : $(u_n)_{n\in\mathbb{N}}$ est divergente.

Exemple 3.3.6.6 Soit (u_n) définie par : $\forall n \in \mathbb{N}^\star$, $u_n = \sum\limits_{k=1}^{n} \dfrac{1}{k}$. Pour tout entier $n \geqslant 1$:

$$u_{2n} - u_n = \frac{1}{n+1} + \frac{1}{n+2} + \cdots + \frac{1}{2n} \geqslant n \times \frac{1}{2n} = \frac{1}{2}$$

Si la suite (u_n) converge, alors (u_{2n}) converge aussi et $\lim\limits_{n\to+\infty} u_{2n} = \lim\limits_{n\to+\infty} u_n$. Mais alors, $(u_{2n} - u_n)$ converge vers 0 alors que pour tout $n \geqslant 1$, $u_{2n} - u_n \geqslant \frac{1}{2}$. C'est absurde et donc la suite (u_n) diverge.

Remarques : *dans l'exemple précédent,*

- *on pouvait aussi montrer par récurrence que :* $\forall n \geqslant 1$, $u_{2^n} \geqslant 1 + \frac{n}{2}$. *Par conséquent,* (u_n) *n'est pas majorée, donc n'est pas bornée et par suite, n'est pas convergente ;*
- *on verra un peu plus loin (théorème de la limite monotone) que puisque* (u_n) *est croissante et ne converge pas, nécessairement* $\lim\limits_{n\to+\infty} u_n = +\infty$ *;*
- *on verra aussi un peu plus loin (paragraphes 3.4.2 et 3.5.4) comment trouver un équivalent de* u_n *;*
- *enfin, la suite* $(u_n)_{n\geqslant 1}$ *est souvent notée* (H_n) *et s'appelle la série harmonique.*

À propos des suites extraites des termes pairs et impairs, la proposition suivante est souvent utile.

Proposition 3.3.6.7 *Soit* $(u_n)_{n\in\mathbb{N}}$ *une suite de nombres réels. On suppose que les suites* (u_{2n}) *et* (u_{2n+1}) *convergent vers la même limite* ℓ*. Alors, la suite* $(u_n)_{n\in\mathbb{N}}$ *est convergente de limite* ℓ*.*

Preuve :

« Moralement » c'est évident car les termes d'indices pairs sont aussi proche que l'on veut de ℓ tout comme les termes d'indices impairs. Formellement, soit $\varepsilon > 0$. Puisque (u_{2n}) et (u_{2n+1}) convergent vers ℓ, il existe deux entiers naturels n_1 et n_2 tels que :

$$\forall n \geqslant n_1 \ , \ |u_{2n} - \ell| \leqslant \varepsilon \quad \text{et } \forall n \geqslant n_2 \ , \ |u_{2n+1} - \ell| \leqslant \varepsilon$$

Posons alors $n_0 = \max(2n_1, 2n_2 + 1)$. Soit $n \in \mathbb{N}$ tel que $n \geqslant n_0$.

- Si n est pair, alors il existe $k \in \mathbb{N}$ tel que $n = 2k$ et par hypothèse, $2k = n \geqslant n_0 \geqslant 2n_1$, c'est-à-dire $k \geqslant n_1$. Alors, d'après la relation ci-dessus, $|u_{2k} - \ell| \leqslant \varepsilon$, c'est-à-dire $|u_n - \ell| \leqslant \varepsilon$.
- On montre de même que si n est impair, alors $|u_n - \ell| \leqslant \varepsilon$.

Ainsi, pour tout entier $n \geqslant n_0$, $|u_n - \ell| \leqslant \varepsilon$. Ce qui prouve que $(u_n)_{n\in\mathbb{N}}$ converge vers ℓ.

⊠

⚠ **Attention :** il ne faut pas oublier que dans cette proposition, on suppose que (u_{2n}) et (u_{2n+1}) convergent et ont la même limite ! On peut très bien avoir (u_{2n}) et (u_{2n+1}) qui convergent bien que (u_n) soit divergente ! C'est le cas par exemple pour la suite $((-1)^n)$.

Exercice 3.3.6.8 Soit (u_n) une suite réelle. On suppose que (u_{3n}), (u_{3n+1}) et (u_{3n+2}) convergent.

1. Montrer que si ces trois suites extraites ont la même limite, alors (u_n) converge.
2. Montrer à l'aide d'un contre-exemple que la suite (u_n) n'est pas nécessairement convergente.

Exercice 3.3.6.9 Comment peut-on généraliser la proposition ou le résultat de l'exercice précédent ?

Remarque : *terminons cette partie sur le lien entre la convergence d'une suite et de suites extraites par quelques petites remarques :*

- *il est possible qu'une suite n'ait aucune suite extraite convergente. Par exemple, si (u_n) diverge vers $+\infty$, alors toute suite extraite de (u_n) diverge (vers $+\infty$) ;*
- *même si la suite (u_n) n'a pas de limite, il est possible qu'aucune suite extraite de (u_n) converge. Par exemple, la suite (u_n) définie par : $\forall n \in \mathbb{N}$, $u_n = (-1)^n \times n$. Cette suite n'a pas de limite (car (u_{2n}) et (u_{2n+1}) ont des limites différentes) et une suite extraite de (u_n) est soit divergente (sans limite), soit divergente de limite $+\infty$ (c'est le cas lorsque l'extraction φ ne prend que des valeurs paires à partir d'un certain rang), soit divergente de limite $-\infty$ (c'est le cas lorsque l'extraction φ ne prend que des valeurs impaires à partir d'un certain rang) ;*
- *on verra un peu plus loin qu'une suite réelle admet toujours au moins une suite extraite qui a une limite : soit la suite (u_n) n'est pas majorée et on montre alors qu'il existe une suite extraite qui tend vers $+\infty$ (voir les exercices à la fin du chapitre), soit (u_n) n'est pas minorée et on montre qu'il existe une suite extraite qui tend vers $-\infty$ ou bien (u_n) est bornée et il existe une suite extraite qui converge (théorème de Bolzano-Weierstrass, voir paragraphe 3.4.4) ;*
- *une suite (u_n) peut avoir des suites extraites qui convergent vers des valeurs différentes. Il peut y avoir un nombre fini arbitraire (c'est-à-dire aussi grand que l'on veut) de limites différentes, ou même une infinité. Par exemple,*
  - *si $p \in \mathbb{N}^\star$ est fixé, pour la suite (u_n) définie par : $\forall n \in \mathbb{N}$, $u_n = \cos\left(\frac{n\pi}{p}\right)$, les suites $(u_{2np+r})_{n\in\mathbb{N}}$ pour $r \in [\![0, 2p-1]\!]$ convergent (chacune est constante égale à $\ell_r = \cos(\frac{r\pi}{p})$). Les valeurs de ℓ_r pour $0 \leqslant r \leqslant p$ sont deux à deux distinctes (et on peut montrer que ce sont les seules limites possibles pour une suite extraite convergente) ;*
  - *pour la suite $(u_n) = (\cos(n))$, on a vu dans l'exercice 2.4.8.3, que tout élément de $[-1, 1]$ est la limite d'une suite extraite.*

3.3.7 Caractérisation de la densité par les suites

Théorème 3.3.7.1 *Soit A une partie de $\mathbb{R}$. Alors les énoncés suivants sont équivalents :*

(i) A est dense dans $\mathbb{R}$;

(ii) tout nombre réel est limite d'une suite d'éléments de A, c'est-à-dire

$$\forall x \in \mathbb{R}\ ,\ \exists (a_n) \in A^{\mathbb{N}}\ ,\ \lim_{n\to+\infty} a_n = x$$

On dit que (ii) est la caractérisation séquentielle (ou par les suites) de la densité.

Preuve :

• $(i) \Longrightarrow (ii)$

On suppose que A est dense dans $\mathbb{R}$.

Soit $x \in \mathbb{R}$. Par définition de la densité de A dans $\mathbb{R}$, pour tout entier $n \in \mathbb{N}$, $]x - \frac{1}{n+1}, x + \frac{1}{n+1}[\cap A \neq \emptyset$: soit $a_n \in]x - \frac{1}{n+1}, x + \frac{1}{n+1}[\cap A$. Ceci définit une suite $(a_n)_{n\in\mathbb{N}}$ d'éléments de A qui vérifie :

$$\forall n \in \mathbb{N}\ ,\ |x - a_n| \leqslant \frac{1}{n+1}$$

D'après le théorème des gendarmes, $\lim_{n\to+\infty} a_n = x$, prouvant ainsi (ii).

• $(ii) \Longrightarrow (i)$

On suppose (ii). Montrons que A est dense dans $\mathbb{R}$. Soient a et b deux réels tels que $a < b$. Posons $x = \frac{a+b}{2}$. D'après (ii), il existe une suite $(a_n)_{n\in\mathbb{N}} \in A^{\mathbb{N}}$ telle que $\lim_{n\to+\infty} a_n = x$.
Soit $\varepsilon = \frac{b-a}{4}$. Par définition de la convergence, il existe un entier n_0 tel que :

$$\forall n \geqslant n_0\ ,\ |a_n - x| \leqslant \varepsilon$$

On a alors :

$$a < \frac{a+b}{2} - \frac{b-a}{4} \leqslant a_{n_0} \leqslant \frac{a+b}{2} + \frac{b-a}{4} < b$$

Par suite, $a_{n_0} \in A \cap]a, b[$ et donc $A \cap]a, b[\neq \emptyset$. Ce qui prouve que A est dense dans $\mathbb{R}$.

⊠

Remarque : *en utilisant cette caractérisation, on a vu qu'il est assez simple de prouver que* $\mathbb{Q}$ *et* $\mathbb{R} \setminus \mathbb{Q}$ *sont denses dans* $\mathbb{R}$.

Exercice 3.3.7.2 Montrer que l'ensemble $\mathbb{D}_2 = \{\frac{p}{2^n} \ , \ (n,p) \in \mathbb{N} \times \mathbb{Z}\}$ est dense dans $\mathbb{R}$.

3.4 Théorèmes d'existence de limite

3.4.1 Théorèmes de convergence et de divergence monotone

Théorème 3.4.1.1 *Soit* $(u_n)_{n\in\mathbb{N}}$ *une suite croissante. Alors, on a les équivalences suivantes :*

$$(u_n)_{n\in\mathbb{N}} \text{ converge} \iff (u_n)_{n\in\mathbb{N}} \text{ est majorée}$$

$$\lim_{n\to+\infty} u_n = +\infty \iff (u_n)_{n\in\mathbb{N}} \text{ n'est pas majorée}$$

De plus, si $(u_n)_{n\in\mathbb{N}}$ *converge, alors* $\lim\limits_{n\to+\infty} u_n = \sup\{u_n \ , \ n \in \mathbb{N}\} = \sup\limits_{n\in\mathbb{N}} u_n$.

De façon analogue, si $(v_n)_{n\in\mathbb{N}}$ *est décroissante, alors :*

$$(v_n)_{n\in\mathbb{N}} \text{ converge} \iff (v_n)_{n\in\mathbb{N}} \text{ est minorée}$$

$$\lim_{n\to+\infty} v_n = -\infty \iff (v_n)_{n\in\mathbb{N}} \text{ n'est pas minorée}$$

De plus, si $(v_n)_{n\in\mathbb{N}}$ *converge, alors* $\lim\limits_{n\to+\infty} v_n = \inf\{v_n \ , \ n \in \mathbb{N}\} = \inf\limits_{n\in\mathbb{N}} v_n$.

Preuve :

Tout d'abord, on constate qu'il suffit de traiter le cas où $(u_n)_{n\in\mathbb{N}}$ est croissante (on déduit alors le résultat pour une suite décroissante en introduisant $(-v_n)$).

Par ailleurs, les deux implications directes $\Longrightarrow$ sont évidentes. Il reste donc uniquement à prouver les deux implications réciproques.

• On suppose que $(u_n)_{n\in\mathbb{N}}$ est majorée.

Dans ce cas, $A = \{u_n \ , \ n \in \mathbb{N}\}$ est une partie non vide et majorée de $\mathbb{R}$: elle admet donc une borne supérieure. Soit $\ell = \sup A$. Montrons que $(u_n)_{n\in\mathbb{N}}$ converge vers ℓ.
Soit $\varepsilon > 0$. D'après la caractérisation de la borne supérieure dans $\mathbb{R}$, il existe $a \in A$ tel que : $\ell - \varepsilon < a \leqslant \ell$. Par définition de l'ensemble A, il existe un entier n_0 tel que $a = u_{n_0}$.

On a alors pour tout entier $n \geqslant n_0$:

$$u_{n_0} \leqslant u_n \text{ (puisque } (u_n)_{n\in\mathbb{N}} \text{ est croissante)}$$

et

$$u_n \leqslant \ell \text{ (puisque } u_n \in A \text{ et } \ell = \sup A)$$

Par conséquent,

$$\forall n \geqslant n_0 \ , \ \ell - \varepsilon \leqslant u_{n_0} \leqslant u_n \leqslant \ell$$

Ce qui prouve que $(u_n)_{n\in\mathbb{N}}$ converge vers ℓ.

• On suppose à présent que la suite $(u_n)_{n\in\mathbb{N}}$ n'est pas majorée. Montrons que $\lim\limits_{n\to+\infty} u_n = +\infty$.

Soit $M \in \mathbb{R}$. $(u_n)_{n\in\mathbb{N}}$ n'étant pas majorée, M n'est pas un majorant de la suite, c'est-à-dire qu'il existe un entier n_0 tel que : $u_{n_0} \geqslant M$. La suite $(u_n)_{n\in\mathbb{N}}$ étant croissante, il vient :

$$\forall n \geqslant n_0 \ , \ u_n \geqslant u_{n_0} \geqslant M$$

Ce qui prouve que $(u_n)_{n\in\mathbb{N}}$ diverge vers $+\infty$.

⊠

Remarques : *on déduit immédiatement les deux propriétés suivantes :*

- *si $(u_n)_{n\in\mathbb{N}}$ est croissante et converge vers ℓ, alors $\forall n \in \mathbb{N}$, $u_n \leqslant \ell$;*
- *si $(u_n)_{n\in\mathbb{N}}$ est décroissante et converge vers ℓ, alors $\forall n \in \mathbb{N}$, $u_n \geqslant \ell$.*

Remarque : *on peut aussi reformuler ce théorème (et l'appeler théorème de la limite monotone pour les suites) de la façon suivante : « soit $(u_n)_{n\in\mathbb{N}}$ une suite réelle monotone, alors $(u_n)_{n\in\mathbb{N}}$ admet une limite (finie ou infinie) ». Pour être plus précis, on rajoute alors l'énoncé donné avant qui précise clairement quand cette limite est finie et quand elle est infinie.*

Exemple 3.4.1.2 On considère la suite $(u_n)_{n\in\mathbb{N}}$ définie par : $u_0 > 0$ et la relation de récurrence $\forall n \in \mathbb{N}$, $u_{n+1} = \ln(1 + u_n)$.

• Pour commencer, on montre par récurrence immédiate que la suite $(u_n)_{n\in\mathbb{N}}$ est bien définie et que de plus, pour tout entier $n \in \mathbb{N}$, $u_n > 0$.

• La fonction ln est une fonction de référence et on sait que : $\forall x \in]-1, +\infty[$, $\ln(1+x) \leqslant x$. Il s'ensuit que :

$$\forall n \in \mathbb{N} \ , \ u_{n+1} = \ln(1 + u_n) \leqslant u_n$$

autrement dit, la suite $(u_n)_{n\in\mathbb{N}}$ est décroissante.

• Ainsi, la suite $(u_n)_{n\in\mathbb{N}}$ est décroissante et minorée donc, d'après le théorème de la limite monotone, $(u_n)_{n\in\mathbb{N}}$ converge.

• Soit $\ell = \lim_{n\to+\infty} u_n$ (donc on vient de justifier l'existence dans $\mathbb{R}$). Puisque $(u_n)_{n\in\mathbb{N}}$ est minorée par 0, $\ell \geqslant 0$. De plus,

- ∗ d'une part, $(u_{n+1})_{n\in\mathbb{N}}$ converge vers ℓ car c'est une suite extraite de $(u_n)_{n\in\mathbb{N}}$;
- ∗ d'autre part, par continuité de ln [4] au point $1+\ell$, $\lim_{n\to+\infty} \ln(1+u_n) = \ln(1+\ell)$, c'est-à-dire $\lim_{n\to+\infty} u_{n+1} = \ln(1+\ell)$.

Par unicité de la limite, $\ell = \ln(1+\ell)$ et par conséquent $\ell = 0$.

Remarque : *le raisonnement fait dans l'exemple précédent est un raisonnement tout à fait « typique ». Autrement dit, c'est un raisonnement que vous serez souvent amené à reproduire. Il faut bien comprendre qu'il y a deux étapes « indépendantes » : la première est l'existence de la limite (qui sera souvent obtenue en appliquant le théorème de la limite monotone) et la seconde est le calcul de la valeur de cette limite.*

Exercice 3.4.1.3 Soit $(u_n)_{n\in\mathbb{N}}$ définie par $u_0 \in [0, \frac{\pi}{2}]$ et $\forall n \in \mathbb{N}$, $u_{n+1} = \sin(u_n)$. Montrer que $(u_n)_{n\in\mathbb{N}}$ converge puis déterminer sa limite.

Exemple 3.4.1.4 Soit pour $n \geqslant 1$, $H_n = \sum_{k=1}^{n} \frac{1}{k}$. La suite (H_n) est croissante et on a déjà vu que pour tout $n > 0$, $H_{2^n} \geqslant 1 + \frac{n}{2}$. La suite $(H_n)_{n\in\mathbb{N}}$ est donc croissante et non majorée. Par conséquent, elle diverge vers $+\infty$.

Exemple 3.4.1.5 On considère la suite $(W_n)_{n\in\mathbb{N}}$ définie par :

$$\forall n \in \mathbb{N} \ , \ W_n = \int_0^{\frac{\pi}{2}} (\cos(x))^n \, \mathrm{d}x$$

Cette suite est appelée la suite des intégrales de Wallis. On veut montrer que $(W_n)_{n\in\mathbb{N}}$ converge.

• Tout d'abord, on peut remarquer que pour tout entier $n \in \mathbb{N}$, W_n est bien défini car la fonction $x \longmapsto (\cos(x))^n$ est continue sur $[0, \frac{\pi}{2}]$.

• Ensuite, soit $n \in \mathbb{N}$. Pour tout $x \in [0, \frac{\pi}{2}]$, $\cos(x) \in [0, 1]$. Par suite,

$$\forall x \in [0, \frac{\pi}{2}] \ , \ 0 \leqslant (\cos(x))^{n+1} \leqslant (\cos(x))^n$$

Par croissance de l'intégrale,

$$0 \leqslant \int_0^{\frac{\pi}{2}} (\cos(x))^{n+1} \, \mathrm{d}x \leqslant \int_0^{\frac{\pi}{2}} (\cos(x))^n \, \mathrm{d}x$$

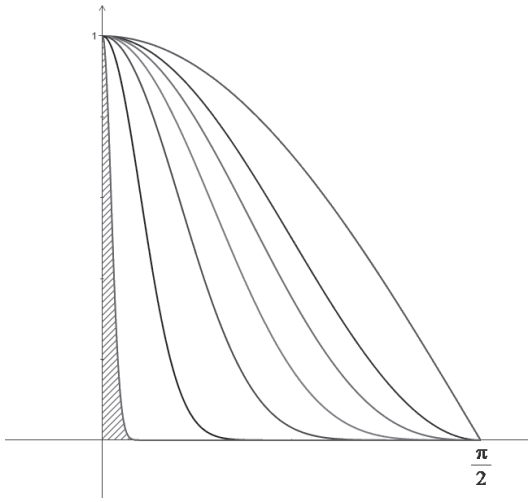
On en déduit donc que :

4. à nouveau, voir la caractérisation séquentielle de la continuité (6.2.4).

∗ la suite $(W_n)_{n\in\mathbb{N}}$ est décroissante ;
∗ et la suite $(W_n)_{n\in\mathbb{N}}$ est minorée (par 0).

D'après le théorème de convergence monotone, $(W_n)_{n\in\mathbb{N}}$ converge.

• Le calcul de limite, ou plus exactement la justification, est un peu plus délicate. Graphiquement, on a la représentation suivante :



Pour $n \in \mathbb{N}$, W_n est l'aire entre la courbe représentative de $x \longmapsto (\cos(x))^n$ et l'axe des abscisses (pour x dans l'intervalle $[0, \frac{\pi}{2}]$). Sur le dessin, on « devine bien » que l'aire devient de plus en plus petite, c'est-à-dire qu'on devine que la suite $(W_n)_{n\in\mathbb{N}}$ converge vers 0.
On va donc le prouver en utilisant la définition de la limite. Soit $\varepsilon \in]0, \frac{\pi}{2}[$ et soit $n \in \mathbb{N}$.

$$\begin{aligned}\int_0^{\frac{\pi}{2}} (\cos(x))^n \,\mathrm{d}x &= \int_0^{\varepsilon} (\cos(x))^n \,\mathrm{d}x + \int_{\varepsilon}^{\frac{\pi}{2}} (\cos(x))^n \,\mathrm{d}x \\ &\leqslant \int_0^{\varepsilon} 1 \,\mathrm{d}x + \int_{\varepsilon}^{\frac{\pi}{2}} (\cos(\varepsilon))^n \,\mathrm{d}x \\ &\leqslant \varepsilon + \left(\frac{\pi}{2} - \varepsilon\right)(\cos(\varepsilon))^n\end{aligned}$$

Or, $|\cos(\varepsilon)| < 1$ donc $\lim\limits_{n\to+\infty} \left(\left(\frac{\pi}{2} - \varepsilon\right)(\cos(\varepsilon))^n\right) = 0$. Il existe un entier $n_0 \in \mathbb{N}$ tel que :

$$\forall n \geqslant n_0 \ , \ \left|\left(\frac{\pi}{2} - \varepsilon\right)(\cos(\varepsilon))^n\right| \leqslant \varepsilon$$

Alors, pour tout entier $n \geqslant n_0$, $0 \leqslant W_n \leqslant 2\varepsilon$. Ainsi, $(W_n)_{n\in\mathbb{N}}$ converge vers 0.

Remarque : *vous reverrez ces intégrales de Wallis dans les cours d'intégration (cours de mathématiques supérieures 2 et cours de mathématiques spéciales 2). Avec des outils un peu plus avancé, vous verrez qu'il est facile de prouver la convergence vers* 0 *et même de trouver un équivalent.*

3.4.2 Application du théorème de la limite monotone aux séries à termes positifs

Soit $(u_n)_{n\in\mathbb{N}}$ une suite réelle. On pose alors :

$$\forall n \in \mathbb{N}\ ,\ S_n = \sum_{k=0}^{n} u_k = u_0 + u_1 + \cdots + u_n$$

Définition 3.4.2.1 Soit $(u_n)_{n\in\mathbb{N}}$ une suite réelle. On appelle série (ou série réelle) de terme général u_n la suite $(S_n)_{n\in\mathbb{N}}$ et on la note aussi $\sum u_n$.
Pour $n \in \mathbb{N}$ donné, le nombre S_n est appelé la somme partielle d'ordre n de la série.

Remarque importante : *connaître la suite $(u_n)_{n\in\mathbb{N}}$ ou connaître la série de terme général u_n sont équivalents. En effet, avec les notations précédentes,*

$$S_0 = u_0 \quad et \quad \forall n \geqslant 1\ ,\ u_n = S_n - S_{n-1}$$

Définition 3.4.2.2 On dit que la série $\sum u_n$ converge si la suite $(S_n)_{n\in\mathbb{N}}$ est convergente. Dans ce cas, la limite (finie) de la suite $(S_n)_{n\in\mathbb{N}}$ est appelée la somme de la série, et on note :

$$\sum_{n=0}^{+\infty} u_n = \lim_{n\to+\infty} S_n$$

On dit que la série $\sum u_n$ est divergente (ou diverge) si $(S_n)_{n\in\mathbb{N}}$ est divergente.

⚠ **Attention :** il est strictement interdit d'utiliser la notation $\sum_{n=0}^{+\infty} u_n$ avant d'avoir prouvé la convergence de la série $\sum u_n$, c'est-à-dire la convergence de la suite $(S_n)_{n\in\mathbb{N}}$ des sommes partielles !

Exemple 3.4.2.3 On a montré que la suite (H_n) diverge vers $+\infty$. Avec le vocabulaire des séries, ceci signifie que la série de terme général $u_n = \frac{1}{n+1}$ est une série divergente.

Exemple 3.4.2.4 Soit $q \in]-1,1[$. Alors la série de terme général q^n est convergente et sa somme vaut $\dfrac{1}{1-q}$. En effet, pour tout entier n, la somme partielle d'ordre n est :

$$S_n = \sum_{k=0}^{n} q^k = \frac{1-q^{n+1}}{1-q} \quad \text{(puisque } q \neq 1\text{)}$$

Or, comme $|q| < 1$, $\lim\limits_{n\to+\infty} q^n = 0$. Par suite, $\lim\limits_{n\to+\infty} S_n = \dfrac{1}{1-q}$. On écrira donc :

$$\sum_{n=0}^{\infty} q^n = \frac{1}{1-q}$$

On dit que $\sum q^k$ est la série géométrique de raison q.

Exemple 3.4.2.5 La série $\sum(-1)^n$ est une série divergente. En effet, si on note (S_n) la suite des sommes partielles, alors pour tout entier $n \in \mathbb{N}$, $S_{2n} = 1$ et $S_{2n+1} = 0$. Les suites extraites (S_{2n}) et (S_{2n+1}) convergent vers des limites différentes donc (S_n) diverge.

Dans ce livre, on ne va pas étudier les séries en général, ni même établir les propriétés générales (et simples) de certains types de séries. On va se contenter d'un seul résultat. Ceci n'est donc qu'une brève introduction aux séries qui seront étudiées plus en détails dans les cours de mathématiques supérieures 2 et spéciales 1.

Proposition 3.4.2.6 *Soit $\sum u_n$ une série à termes positifs (c'est-à-dire que pour tout entier n, $u_n \geqslant 0$). Alors :*

$$\sum u_n \quad \textit{converge} \iff (S_n)_{n\in\mathbb{N}} \textit{ est majorée}$$

Preuve :

En effet, pour tout entier n, $S_{n+1} - S_n = u_{n+1} \geqslant 0$ (puisque (u_n) est positive par hypothèse) donc la suite $(S_n)_{n\in\mathbb{N}}$ est croissante.
D'après le théorème de convergence monotone, $(S_n)_{n\in\mathbb{N}}$ converge si et seulement si elle est majorée.

⊠

⚠ **Attention :** ce résultat est faux si on retire l'hypothèse « à termes positifs ». En effet, si $u_n = (-1)^n$, alors la suite $(S_n)_{n\in\mathbb{N}}$ est clairement majorée par 1 et pourtant $(S_n)_{n\in\mathbb{N}}$ diverge.

Exemple 3.4.2.7 On considère la série $\sum \frac{1}{(n+1)^2}$. Pour tout entier $n \in \mathbb{N}^\star$,

$$\frac{1}{(n+1)^2} \leqslant \frac{1}{n(n+1)} = \frac{1}{n} - \frac{1}{n+1}$$

Par suite, pour $n \in \mathbb{N}^\star$,

$$\sum_{k=0}^{n} \frac{1}{(k+1)^2} = 1 + \sum_{k=1}^{n} \frac{1}{(k+1)^2} \leqslant 1 + \sum_{k=1}^{n} \left(\frac{1}{k} - \frac{1}{(k+1} \right) = 2 - \frac{1}{n+1}$$

On en déduit donc que : $\forall n \in \mathbb{N}^\star$, $\displaystyle\sum_{k=0}^{n} \frac{1}{(k+1)^2} \leqslant 2$, ce qui prouve que la suite des sommes partielles de cette série est majorée (par 2). On en déduit donc que cette série converge.

Remarque : *les séries de la forme $\sum \frac{1}{n^\alpha}$ avec $\alpha \in \mathbb{R}$ sont appelés les séries de Riemann. Lorsqu'elle est définie, la somme de cette série est notée $\zeta(\alpha)$ et la fonction $\alpha \longmapsto \zeta(\alpha)$ est appelée fonction zêta de Riemann.*
L'exemple précédent montre que $\zeta(2)$ est bien défini et que $\zeta(2) \leqslant 2$. On verra plus tard qu'en fait $\zeta(2) = \frac{\pi^2}{6}$, valeur de référence que vous devez connaître.

Une méthode absolument fondamentale pour l'étude des séries est la méthode de comparaison avec une intégrale. Dans ce paragraphe, on ne donne pas les théorèmes (qui seront étudiés dans le chapitre sur les séries du cours de mathématiques supérieures 2). L'objectif est seulement d'introduire la méthode et de comprendre à travers l'étude d'exemples comment cette technique peut être utilisée pour étudier la convergence d'une série mais aussi dans de nombreux cas d'obtenir une « bonne idée du comportement de S_n », c'est-à-dire de trouver un équivalent lorsque la série diverge ou bien un équivalent de $S_n - \lim\limits_{n\to+\infty} S_n$ lorsque la série converge.

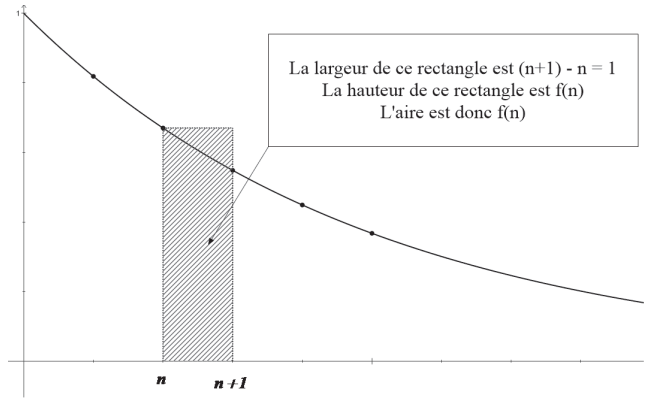
Méthode de comparaison avec une intégrale

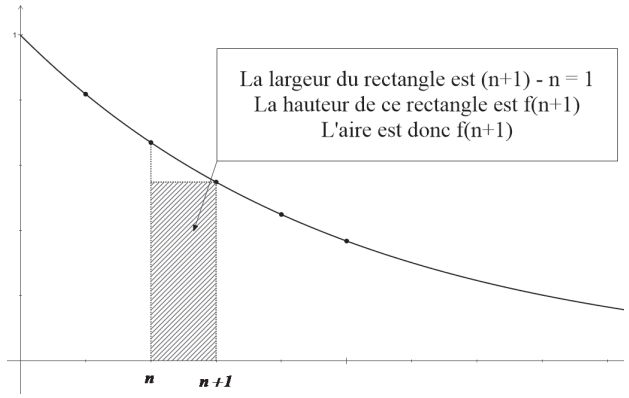
Cadre : on veut étudier une série de la forme $\sum u_n$ où $u_n = f(n)$, f est une fonction.

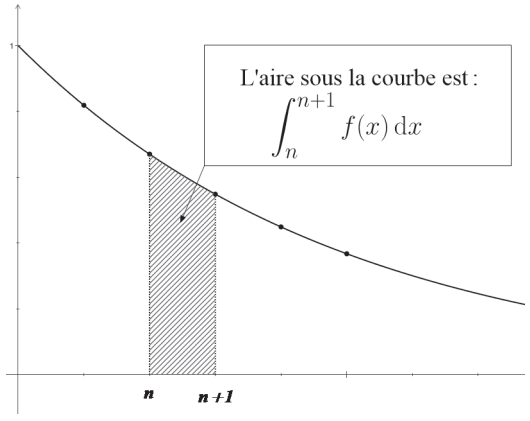
Principe : on veut comparer $f(n)$ avec $\displaystyle\int_n^{n+1} f(x)\,\mathrm{d}x$.

Condition pratique pour appliquer cette méthode : f est monotone.

L'hypothèse f monotone est simplement pour garantir que la seconde étape (c'est-à-dire la comparaison de $f(n)$ avec l'intégrale de f sur $[n, n+1]$) soit simple à faire comme on peut le comprendre avec les figures suivantes (cas où f est décroissante) :







On va donc pouvoir encadrer $f(n)$ par des intégrales et en sommant, comparer la somme partielle S_n avec une intégrale de la fonction f.

La raison pour laquelle on suppose que f est monotone est que sinon, on ne peut pas comparer la valeur de $\displaystyle\int_n^{n+1} f(x)\,\mathrm{d}x$ avec $f(n)$ (et $f(n+1)$).

On va mettre en œuvre cette méthode sur l'exemple précédent avec la série harmonique, c'est-à-dire $\sum \frac{1}{n}$. On pose pour $n \geqslant 1$, $u_n = \frac{1}{n}$ et on appelle $(S_n)_{n\in\mathbb{N}}$ la série de terme général u_n.

Considérons la fonction inverse $f : x \longmapsto \frac{1}{x}$. Soit $k \in \mathbb{N}^\star$. f est décroissante (strictement) sur $]0, +\infty[$ donc :

$$\forall x \in [k, k+1]\ ,\ \frac{1}{k+1} \leqslant \frac{1}{x} \leqslant \frac{1}{k}$$

Par croissance de l'intégrale, on a alors :

$$\int_k^{k+1} \frac{\mathrm{d}x}{k+1} \ \leqslant\ \int_k^{k+1} \frac{\mathrm{d}x}{x} \ \leqslant\ \int_k^{k+1} \frac{\mathrm{d}x}{k}$$

Puisque k et $k+1$ sont des constantes, on obtient :

$$\frac{1}{k+1}\left((k+1)-k\right) \leqslant \int_k^{k+1} \frac{\mathrm{d}x}{x} \leqslant \frac{1}{k}\left((k+1)-k\right)$$

c'est-à-dire

$$\forall k \in \mathbb{N}^\star\ ,\ \frac{1}{k+1} \leqslant \int_k^{k+1} \frac{\mathrm{d}x}{x} \leqslant \frac{1}{k} \quad \text{ou encore} \quad \forall k \in \mathbb{N}^\star\ ,\ u_{k+1} \leqslant \int_k^{k+1} \frac{\mathrm{d}x}{x} \leqslant u_k$$

Soit alors $n \geqslant 2$. On somme les inégalités précédentes pour k compris entre 1 et $n-1$, ce qui donne :

$$\sum_{k=1}^{n-1} u_{k+1} \ \leqslant\ \sum_{k=1}^{n-1} \int_k^{k+1} \frac{\mathrm{d}x}{x} \ \leqslant \sum_{k=1}^{n-1} u_k$$

D'après la relation de Chasles pour les intégrales (c'est-à-dire $\int_a^b f + \int_b^c f = \int_a^c f$), on a alors :

$$\sum_{j=2}^{n} u_j \leqslant \int_1^n \frac{\mathrm{d}x}{x} \leqslant \sum_{k=1}^{n-1} u_k$$

soit encore,

$$S_n - 1 \leqslant \ln(n) \leqslant S_n - \frac{1}{n}$$

Il s'ensuit que :

$$\ln(n) + \frac{1}{n} \leqslant S_n \leqslant \ln(n) + 1$$

Ceci nous permet immédiatement de déterminer la limite de (S_n) mais surtout, ceci permet de déterminer le comportement précis de (u_n). En appliquant le théorème des gendarmes, on obtient :

$$\lim_{n\to+\infty} \frac{S_n}{\ln(n)} = 1 \quad \text{ce qu'on notera} \quad S_n \underset{n\to+\infty}{\sim} \ln(n)$$

À retenir : une méthode pour obtenir des informations sur une série à termes positifs de la forme $\sum f(n)$ est de comparer les sommes partielles avec une intégrale. Cette méthode s'applique lorsque f est une fonction croissante (ou bien décroissante) sur un certain intervalle $[A, +\infty[$ avec $A \geqslant 0$.

Méthode :

1. on encadre l'intégrale $\int_n^{n+1} f(x)\,\mathrm{d}x$ avec les valeurs $f(n)$ et $f(n+1)$;
2. on somme les inégalités (une somme finie bien entendu) ;
3. on encadre S_n à l'aide de $\displaystyle\int_1^n f(x)\,\mathrm{d}x$;
4. on calcule $\displaystyle\int_1^n f(x)\,\mathrm{d}x$;
5. on détermine la nature (convergente ou divergente) de S_n (soit on peut majorer S_n et la série sera convergente, soit on obtient une minoration par une suite qui tend vers $+\infty$ et on conclut que (S_n) diverge vers $+\infty$) ;
6. si la série diverge, on essaye d'appliquer le théorème des gendarmes pour déterminer un équivalent de S_n ;
7. si la série converge, on encadre $S_n - \lim\limits_{n\to+\infty} S_n$ par des intégrales et on essaye d'appliquer le théorème des gendarmes pour trouver un équivalent.

Remarque : *évidemment, cette méthode ne s'applique pas à toutes les séries à termes positifs.*

Exemple 3.4.2.8 On considère la série $\sum \frac{1}{\sqrt{n}}$. Notons f la fonction $x \longmapsto \frac{1}{\sqrt{x}}$ de sorte que $\sum \frac{1}{\sqrt{n}} = \sum f(n)$.

Étape 1 : encadrement par une intégrale

La fonction $x \longmapsto \frac{1}{\sqrt{x}}$ est une fonction continue et décroissante sur $[1, +\infty[$. Soit $k \in \mathbb{N}^\star$.

$$\forall x \in [k, k+1]\ ,\ f(k+1) \leqslant f(x) \leqslant f(k)$$

D'où l'on déduit que :

$$f(k+1) \leqslant \int_k^{k+1} f(x)\,\mathrm{d}x \leqslant f(k)$$

Étapes 2 et 3 : on somme les inégalités et on encadre S_n par une intégrale

Soit $n \in \mathbb{N}$ tel que $n \geqslant 2$. On somme les inégalités précédentes pour $k \in [\![1, n-1]\!]$, ce qui donne :

$$\sum_{k=1}^{n-1} f(k+1) \leqslant \sum_{k=1}^{n-1} \int_k^{k+1} f(x)\,\mathrm{d}x \leqslant \sum_{k=1}^{n-1} f(k)$$

soit encore

$$\sum_{j=2}^{n} f(j) \leqslant \int_1^n f(x)\,\mathrm{d}x \leqslant \sum_{k=1}^{n} f(k) - f(n)$$

En notant $S_n = \displaystyle\sum_{k=1}^{n} \frac{1}{\sqrt{k}} = \sum_{k=1}^{n} f(k)$ la somme partielle d'ordre n de la série, on a donc :

$$S_n - f(1) \leqslant \int_1^n f(x)\,\mathrm{d}x \leqslant S_n - f(n)$$

et donc finalement,

$$\forall n \geqslant 2\ ,\ \int_1^n f(x)\,\mathrm{d}x + f(n) \leqslant S_n \leqslant \int_1^n f(x)\,\mathrm{d}x + f(1)$$

Étape 4 : on calcule l'intégrale obtenue

Pour $n \in \mathbb{N}^\star$, $\displaystyle\int_1^n f(x)\,\mathrm{d}x = \int_1^n \frac{\mathrm{d}x}{\sqrt{x}} = 2\sqrt{n} - 2$. Par suite,

$$\forall n \geqslant 2\ ,\ 2\sqrt{n} - 2 + \frac{1}{\sqrt{n}} \leqslant S_n \leqslant 2\sqrt{n} - 1$$

Étape 5 : on détermine la nature (convergente/divergente) de la série

Puisque $\displaystyle\lim_{n\to+\infty} \left(2\sqrt{n} - 2 + \frac{1}{\sqrt{n}}\right) = +\infty$, d'après les règles de comparaison pour les suites,

$$\lim_{n\to+\infty} S_n = +\infty$$

Ce qui prouve que la série $\sum \frac{1}{\sqrt{n}}$ diverge.

Étape 6/7 : on cherche un « équivalent » de S_n (car la série diverge)

D'après ce qui précède,

$$\forall n \geqslant 2\ ,\ 1 - \frac{1}{\sqrt{n}} + \frac{1}{2n} \leqslant \frac{S_n}{2\sqrt{n}} \leqslant 1 - \frac{1}{2\sqrt{n}}$$

Or, $\displaystyle\lim_{n\to+\infty} \left(1 - \frac{1}{\sqrt{n}} + \frac{1}{2n}\right) = \lim_{n\to+\infty} \left(1 - \frac{1}{2\sqrt{n}}\right) = 1$. D'après le théorème des gendarmes, la suite $(\frac{S_n}{2\sqrt{n}})$ converge et :

$$\lim_{n\to+\infty} \frac{S_n}{2\sqrt{n}} = 1$$

Remarque : *la divergence de cette série est en réalité évidente car pour tout entier $n \geqslant 1$,*

$$\sum_{k=1}^{n} \frac{1}{\sqrt{k}} \geqslant n \times \frac{1}{\sqrt{n}} = \sqrt{n}$$

(on minore par le plus petit terme de la somme fois le nombre de termes). Vous verrez dans le cours de mathématiques spéciales 1 d'autres méthodes plus rapides pour trouver un équivalent de la somme partielle.

Exemple 3.4.2.9 On considère la série $\sum \frac{1}{n(\ln(n))^2}$ (définie à partir du rang $n = 2$).

La fonction $x \longmapsto \dfrac{1}{x(\ln(x))^2}$ est continue sur $[2, +\infty[$ et on vérifie que cette fonction est décroissante sur $[2, +\infty[$.

Étape 1 : encadrement du terme général

Soit $n \in \mathbb{N}$ tel que $n \geqslant 2$. On a alors :

$$\forall x \in [n, n+1] \ , \ \frac{1}{(n+1)(\ln(n+1))^2} \leqslant \frac{1}{x(\ln(x))^2} \leqslant \frac{1}{n(\ln(n))^2}$$

Par croissance de l'intégrale, on a alors :

$$\frac{1}{(n+1)(\ln(n+1))^2} \leqslant \int_n^{n+1} \frac{\mathrm{d}x}{x(\ln(x))^2} \leqslant \frac{1}{n(\ln(n))^2}$$

Étapes 2 et 3 : on encadre la somme partielle

Soit $N \in \mathbb{N}$ avec $N \geqslant 3$. On somme les inégalités précédentes pour $n \in [\![2, N-1]\!]$, ce qui donne :

$$\sum_{n=3}^{N} \frac{1}{n(\ln(n))^2} \leqslant \int_2^N \frac{\mathrm{d}x}{x(\ln(x))^2} \leqslant \sum_{n=2}^{N-1} \frac{1}{n(\ln(n))^2}$$

soit encore

$$\int_2^N \frac{\mathrm{d}x}{x(\ln(x))^2} + \frac{1}{N(\ln(N))^2} \leqslant \sum_{n=2}^{N} \frac{1}{n(\ln(n))^2} \leqslant \int_2^N \frac{\mathrm{d}x}{x(\ln(x))^2} + \frac{1}{2(\ln(2))^2}$$

Étape 4 : on calcule l'intégrale

Notons pour $x \geqslant 2$, $u(x) = \ln(x)$. La fonction u est de classe $\mathcal{C}^1$ sur $[2, +\infty[$ et pour tout $x \geqslant 2$,

$$\frac{1}{x(\ln(x))^2} = \frac{u'(x)}{u(x)^2} = \left(-\frac{1}{u}\right)'(x)$$

Il s'ensuit que :

$$\int_2^N \frac{\mathrm{d}x}{x(\ln(x))^2} = \left[-\frac{1}{\ln(x)}\right]_2^N = \frac{1}{\ln(2)} - \frac{1}{\ln(N)}$$

Étape 5 : on détermine la nature de la série

D'après ce qui précède, pour tout entier $N \geqslant 3$,

$$\sum_{n=2}^{N} \frac{1}{n(\ln(n))^2} \leqslant \frac{1}{\ln(2)} - \frac{1}{\ln(N)} + \frac{1}{2(\ln(2))^2} \leqslant \frac{1}{\ln(2)} + \frac{1}{2(\ln(2))^2}$$

Par conséquent, la série $\sum \frac{1}{n(\ln(n))^2}$ est une série à termes positifs dont la suite des sommes partielles est majorée : il s'ensuit que $\sum \frac{1}{n(\ln(n))^2}$ converge. On note $\ell = \displaystyle\sum_{n=2}^{+\infty} \frac{1}{n(\ln(n))^2}$.

Étape 6/7 : on détermine un « équivalent » de $(\ell - S_n)$.

Soient N un entier supérieur ou égal à 3 et $p \geqslant N$. En sommant les inégalités obtenues à la première étape pour $n \in [\![N, p]\!]$, on obtient :

$$\sum_{n=N+1}^{p+1} \frac{1}{n(\ln(n))^2} \leqslant \int_N^{p+1} \frac{\mathrm{d}x}{x(\ln(x))^2} \leqslant \sum_{n=N}^{p} \frac{1}{n(\ln(n))^2}$$

soit encore :

$$\sum_{n=2}^{p+1} \frac{1}{n(\ln(n))^2} - \sum_{n=2}^{N} \frac{1}{n(\ln(n))^2} \leqslant \frac{1}{\ln(N)} - \frac{1}{\ln(p+1)} \leqslant \sum_{n=2}^{p} \frac{1}{n(\ln(n))^2} - \sum_{n=2}^{N-1} \frac{1}{n(\ln(n))^2}$$

En notant pour $(S_n)_{n\geqslant 2}$ la suite des sommes partielles, on a donc :

$$S_{p+1} - S_N \leqslant \frac{1}{\ln(N)} - \frac{1}{\ln(p+1)} \leqslant S_p - S_{N-1}$$

Or, $\lim\limits_{p\to+\infty} \dfrac{1}{\ln(N)} - \dfrac{1}{\ln(p+1)} = \dfrac{1}{\ln(N)}$ et on vient de prouver que $(S_p)_{p\geqslant 2}$ converge. Par suite, chaque terme de l'inégalité précédente admet une limite finie quand p tend vers $+\infty$. On peut donc passer à la limite quand p tend vers $+\infty$ dans l'inégalité, ce qui donne :

$$\ell - S_N \leqslant \frac{1}{\ln(N)} \leqslant \ell - S_{N-1}$$

On en déduit donc que pour tout entier $N \geqslant 3$,

$$\ell - S_N \leqslant \frac{1}{\ln(N)} \leqslant \ell - \left(S_N - \frac{1}{N(\ln(N))^2}\right)$$

c'est-à-dire

$$\frac{1}{\ln(N)} - \frac{1}{N(\ln(N))^2} \leqslant \ell - S_N \leqslant \frac{1}{\ln(N)}$$

Par conséquent, pour tout entier $N \geqslant 3$,

$$1 - \frac{1}{N\ln(N)} \leqslant \ln(N) \times (\ell - S_N) \leqslant 1$$

Or, $\lim\limits_{N\to+\infty} \left(1 - \frac{1}{N\ln(N)}\right) = 1$ donc d'après le théorème des gendarmes :

$$\lim_{N\to+\infty} \ln(N) \times (\ell - S_N) = 1$$

Remarques :

- *on reverra un peu plus loin que dans le dernier exemple, la conclusion s'écrit* $\ell - S_n \underset{n\to+\infty}{\sim} \frac{1}{\ln(n)}$ *;*
- *dans la pratique, lorsque l'on rédige, on n'écrit pas « étape 1 », « étape 2 » etc ;*
- *quand on applique cette méthode (qui est en fait relativement simple), la seule étape qui en réalité peut poser problème est « l'étape 4 », c'est-à-dire le calcul de l'intégrale car souvent on ne sait pas déterminer de primitive de la fonction f. On reverra dans le cours de mathématiques spéciales 2 des techniques plus avancées permettant de soit calculer cette intégrale, soit de donner un équivalent ;*
- *cette technique sera aussi très utilisée pour les séries de fonctions, lorsqu'on cherchera des équivalents de la somme aux bornes de son ensemble de définition ;*
- *enfin, remarquez que cette méthode est souvent un peu longue à rédiger proprement. En particulier, on ne fait pas de passage à la limite (ou des sommes infinies) avant d'avoir justifié l'existence !*

3.4.3 Théorème des suites adjacentes et théorème des segments emboîtés

Définition 3.4.3.1 On dit que deux suites $(u_n)_{n\in\mathbb{N}}$ et $(v_n)_{n\in\mathbb{N}}$ sont adjacentes si l'une est croissante, l'autre décroissante et $\lim\limits_{n\to+\infty} (v_n - u_n) = 0$.

Théorème 3.4.3.2 *Si $(u_n)_{n\in\mathbb{N}}$ et $(v_n)_{n\in\mathbb{N}}$ sont adjacentes, alors $(u_n)_{n\in\mathbb{N}}$ et $(v_n)_{n\in\mathbb{N}}$ convergent vers la même limite. De plus, si $(u_n)_{n\in\mathbb{N}}$ est croissante, alors :*

$$\forall (n,p) \in \mathbb{N}^2 \ , \ u_n \leqslant v_p$$

Preuve :

Quitte à échanger les noms des suites, on peut supposer que $(u_n)_{n\in\mathbb{N}}$ est croissante et $(v_n)_{n\in\mathbb{N}}$ est décroissante.

• Tout d'abord, la suite $(v_n - u_n)_{n\in\mathbb{N}}$ est décroissante de limite nulle. D'après le théorème de convergence monotone, $(v_n - u_n)_{n\in\mathbb{N}}$ est toujours positive, c'est-à-dire que :

$$\forall n \in \mathbb{N} \ , \ u_n \leqslant v_n$$

• D'après ce qui précède, $\forall n \in \mathbb{N} \ , \ u_n \leqslant v_n \leqslant v_0$ puisque la suite $(v_n)_{n\in\mathbb{N}}$ est décroissante. Ainsi, $(u_n)_{n\in\mathbb{N}}$ est croissante et majorée par v_0. Par conséquent, $(u_n)_{n\in\mathbb{N}}$ converge.

• De la même façon, $\forall n \in \mathbb{N} \ , \ u_0 \leqslant u_n \leqslant v_n$. Par conséquent, $(v_n)_{n\in\mathbb{N}}$ est décroissante et minorée par u_0. On en déduit donc que $(v_n)_{n\in\mathbb{N}}$ converge.

• Ayant prouvé que les deux suites convergent, on peut alors écrire que :

$$\lim_{n\to+\infty} u_n - \lim_{n\to+\infty} v_n = \lim_{n\to+\infty} (u_n - v_n) = 0$$

c'est-à-dire que les deux suites convergent vers la même limite.

• Enfin, soient $(n, p) \in \mathbb{N}^2$. D'après la remarque sur les limites des suites monotones, on a :

$$u_n \leqslant \lim_{N\to+\infty} u_N = \lim_{N\to+\infty} v_N \leqslant v_p$$

⊠

Exercice 3.4.3.3 Soient pour $n \geqslant 1$, $u_n = \displaystyle\sum_{k=0}^{n} \frac{1}{k!}$ et $v_n = \displaystyle\sum_{k=0}^{n} \frac{1}{k!} + \frac{1}{n \times n!}$.

1. Montrer que les suites $(u_n)_{n\geqslant 1}$ et $(v_n)_{n\geqslant 1}$ convergent vers une même limite ℓ.
2. On suppose que $\ell = \dfrac{p}{q}$ avec $p, q \in \mathbb{N}^\star$. Montrer que $u_q < \ell < v_q$ puis qu'il existe un entier N tel que $N < p \times q! < N + 1$.
3. On verra plus tard que $\ell = e$. Que vient-on de prouver ?

Remarque : *ce théorème sera à la base du critère spécial pour les séries alternées (que vous verrez dans le cours de mathématiques supérieures 2). En revanche, ce théorème est spécifique aux suites réelles (car on utilise la relation d'ordre dans $\mathbb{R}$) et ne se généralisera pas aux suites complexes (ou aux suites dans un espace vectoriel normé (voir cours de mathématiques spéciales 1)).*

Théorème 3.4.3.4 (Segments emboîtés) *Soit $(I_n)_{n\in\mathbb{N}}$ une suite de segments emboîtés dont le diamètre tend vers 0, c'est-à-dire une suite de segments tels que :*

1. $\forall n \in \mathbb{N}$, $I_{n+1} \subset I_n$;
2. $\lim\limits_{n\to+\infty} diam(I_n) = 0$ *où si* $I = [a, b]$ *avec* $a < b$, $diam(I) = b - a$.

Alors $\bigcap\limits_{n\in\mathbb{N}} I_n$ *est un singleton.*

Preuve :

Pour $n \in \mathbb{N}$, on pose $a_n = \inf I_n$ et $b_n = \sup I_n$, c'est-à-dire $I_n = [a_n, b_n]$.

• Montrons pour commencer que $\bigcap\limits_{n\in\mathbb{N}} I_n \neq \emptyset$

Puisque les segments sont emboîtés, on a :

$$\forall n \in \mathbb{N} \ , \ [a_{n+1}, b_{n+1}] \subset [a_n, b_n]$$

soit encore,

$$\forall n \in \mathbb{N} \ , \ a_n \leqslant a_{n+1} \leqslant b_{n+1} \leqslant b_n$$

On en déduit donc que $(a_n)_{n\in\mathbb{N}}$ est croissante et $(b_n)_{n\in\mathbb{N}}$ est décroissante. Par ailleurs, d'après l'hypothèse 2, $\lim\limits_{n\to+\infty} (b_n - a_n) = 0$.

Ce qui prouve que les suites $(a_n)_{n\in\mathbb{N}}$ et $(b_n)_{n\in\mathbb{N}}$ sont adjacentes. Par conséquent, elles convergent vers une même limite ℓ qui vérifie :

$$\forall n \in \mathbb{N} \ , \ a_n \leqslant \ell \leqslant b_n \quad \text{c'est-à-dire} \quad \forall n \in \mathbb{N} \ , \ \ell \in I_n$$

On en déduit donc que $\ell \in \bigcap\limits_{n\in\mathbb{N}} I_n$.

• Montrons à présent que $\bigcap\limits_{n\in\mathbb{N}} I_n = \{\ell\}$.

Soit $x \in \bigcap\limits_{n\in\mathbb{N}} I_n$. Alors, pour tout entier $n \in \mathbb{N}$, $(x, \ell) \in I_n \times I_n$ donc $\forall n \in \mathbb{N} \ , \ |x - \ell| \leqslant diam(I_n)$ et $\lim\limits_{n\to+\infty} diam(I_n) = 0$. D'après le théorème des gendarmes, $|x - \ell| = 0$, c'est-à-dire $x = \ell$.

⊠

Remarque : *vous verrez plus tard que ce théorème se généralise au théorème des fermés emboîtés.*

3.4.4 Théorème de Bolzano-Weierstrass

Théorème 3.4.4.1 (Bolzano-Weierstrass) *De toute suite réelle bornée on peut extraire une suite convergente.*

Preuve :

Soit $(u_n)_{n\in\mathbb{N}}$ une suite réelle bornée. On note a_0 un minorant de la suite $(u_n)_{n\in\mathbb{N}}$ et b_0 un majorant de la suite $(u_n)_{n\in\mathbb{N}}$. Ces réels existent par hypothèse sur $(u_n)_{n\in\mathbb{N}}$.

Pour (α,β) deux réels tels que $a_0 \leq \alpha \leq \beta \leq b_0$, on note $N(\alpha,\beta)$ l'ensemble des indices $k \in \mathbb{N}$ pour lesquels u_k est compris entre α et β, *i.e.* $N(\alpha,\beta) = \{k \in \mathbb{N} \ / \ \alpha \leq u_k \leq \beta\}$.

• Construisons par récurrence des suites $(a_n)_{n\in\mathbb{N}}$ et $(b_n)_{n\in\mathbb{N}}$ telles que pour tout $n \in \mathbb{N}$,
- l'ensemble $N(a_n,b_n)$ est infini ;
- en notant $I_n = [a_n,b_n]$ et $I_{n+1} = [a_{n+1},b_{n+1}]$, on a $I_{n+1} \subset I_n$;
- $diam(I_{n+1}) = \frac{1}{2}diam(I_n)$.

Posons $I_0 = [a_0,b_0]$. Par construction, tous les termes de la suite $(u_n)_{n\in\mathbb{N}}$ appartiennent à I_0, donc $N(a_0,b_0)$ est infini.

Posons $c_0 = \dfrac{a_0+b_0}{2}$.

Puisque $N(a_0,b_0) = N(a_0,c_0) \cup N(c_0,b_0)$, au moins l'un des deux ensembles $N(a_0,c_0)$ ou $N(c_0,b_0)$ est infini.
Si $N(a_0,c_0)$ est infini, on pose $a_1 = a_0$ et $b_1 = c_0$.
Sinon $N(c_0,b_0)$ est infini et on pose $a_1 = c_0$ et $b_1 = b_0$.

Dans les deux cas, on a $diam(I_1) = \frac{1}{2}diam(I_0)$ car $b_1 - a_1 = \dfrac{1}{2}(b_0 - a_0)$.

Soit $n \in \mathbb{N}$ fixé, on suppose construit $I_n = [a_n,b_n]$ tel que $N(a_n,b_n)$ soit infini et on réitère le processus précédent :

Posons $c_n = \dfrac{a_n+b_n}{2}$.

Puisque $N(a_n,b_n) = N(a_n,c_n) \cup N(c_n,b_n)$, au moins l'un des deux ensembles $N(a_n,c_n)$ ou $N(c_n,b_n)$ est infini.
Si $N(a_n,c_n)$ est infini, on pose $a_{n+1} = a_n$ et $b_{n+1} = c_n$.
Sinon $N(c_n,b_n)$ est infini et on pose $a_{n+1} = c_n$ et $b_{n+1} = b_n$.

On a bien construit $I_{n+1} = [a_{n+1},b_{n+1}]$ tel que $N(a_{n+1},b_{n+1})$ soit infini, et on vérifie que I_{n+1} est inclus dans I_n et que $diam(I_{n+1}) = \frac{1}{2}diam(I_n)$ comme précédemment.

• Par construction, pour tout $n \in \mathbb{N}$, $diam(I_n) = \frac{b_0-a_0}{2^n}$ et $I_{n+1} \subset I_n$. On peut donc appliquer le théorème des segments emboîtés à la suite $(I_n)_{n\in\mathbb{N}}$: il existe $\ell \in \mathbb{R}$ tel que $\bigcap_{n\in\mathbb{N}} I_n = \{\ell\}$.

• On construit enfin par récurrence forte une application $\varphi : \mathbb{N} \longrightarrow \mathbb{N}$ strictement croissante telle que pour tout entier $n \in \mathbb{N}$, $\varphi(n) \in N(a_n, b_n)$.

Initialisation :

Posons $\varphi(0) = 0$. Alors $a_0 \leqslant u_0 \leqslant b_0$ et la propriété est vraie au rang 0.

Hérédité :

Soit $n \in \mathbb{N}$ fixé, supposons avoir construit $\varphi(k)$ pour tout $k \in [\![0, n]\!]$. Puisque l'ensemble $N(a_{n+1}, b_{n+1})$ est un sous-ensemble infini de $\mathbb{N}$, l'ensemble $E = \{k \in N(a_{n+1}, b_{n+1}) \,|\, k > \varphi(n)\}$ n'est pas vide, on peut donc par exemple poser $\varphi(n+1) = \min(E)$. Alors d'une part, $\varphi(n+1) > \varphi(n)$ et d'autre part, puisque $\varphi(n+1) \in N(a_{n+1}, b_{n+1})$, $a_{n+1} \leqslant u_{\varphi(n+1)} \leqslant b_{n+1}$. Ce qui prouve que la propriété est vraie au rang $n+1$ et achève la récurrence.

• On a alors pour tout $n \in \mathbb{N}$ $a_n \leq u_{\varphi(n)} \leq b_n$, donc $(u_{\varphi(n)})_{n\in\mathbb{N}}$ converge vers ℓ d'après le théorème des gendarmes car, en reprenant la preuve du théorème des segments emboîtés, les suites $(a_n)_{n\in\mathbb{N}}$ et $(b_n)_{n\in\mathbb{N}}$ sont adjacentes et ont pour limite commune ℓ.

⊠

Exercice 3.4.4.2 On peut également prouver ce résultat en construisant une suite extraite monotone de $(u_n)_{n\in\mathbb{N}}$. Soit $(u_n)_{n\in\mathbb{N}}$ une suite réelle. On considère l'ensemble :

$$A = \{n \in \mathbb{N} \;/\; \forall k \geqslant n \;,\; u_k \geqslant u_n\}$$

1. On suppose que A est infini. Montrer qu'il existe une suite extraite de $(u_n)_{n\in\mathbb{N}}$ qui est croissante.
2. On suppose que A est fini. Montrer qu'il existe une suite extraite de $(u_n)_{n\in\mathbb{N}}$ qui est décroissante.
3. En déduire une autre preuve du théorème de Bolzano-Weierstrass.

⚠ **Attention :** le théorème de Bolzano-Weierstrass ne dit absolument pas qu'une suite réelle bornée converge ! Il affirme qu'on peut extraire une suite qui converge !

Exercice 3.4.4.3 (Difficile) Soit $(u_n)_{n\in\mathbb{N}}$ une suite réelle bornée vérifiant : si (v_n) et (w_n) sont deux suites extraites de (u_n) qui convergent, alors elles ont la même limite. Montrer que $(u_n)_{n\in\mathbb{N}}$ converge.

3.5 Relations de comparaison

3.5.1 Suites dominées ou négligeables par rapport à une autre

Définition 3.5.1.1 Soient $(u_n)_{n\in\mathbb{N}}$ et $(v_n)_{n\in\mathbb{N}}$ deux suites de nombres réels.

- On dit que la suite $(v_n)_{n\in\mathbb{N}}$ est dominée par la suite $(u_n)_{n\in\mathbb{N}}$, et on note alors $(v_n) = O(u_n)$, si :

$$\exists M \in \mathbb{R} \ , \ \exists N \in \mathbb{N} \ , \ \forall n \geqslant N \ , \ |v_n| \leqslant M|u_n|$$

- On dit que la suite $(v_n)_{n\in\mathbb{N}}$ est négligeable devant $(u_n)_{n\in\mathbb{N}}$, et on note alors $v_n = o(u_n)$, si :

$$\forall \varepsilon > 0 \ , \ \exists N \in \mathbb{N} \ , \ \forall n \geqslant N \ , \ |v_n| \leqslant \varepsilon |u_n|$$

Remarque : *dans le cadre des suites, la notation $(v_n) = O(u_n)$ signifie implicitement que le paramètre n tend vers $+\infty$, ce n'est pas comme pour les fonctions (voir le chapitre 6, paragraphe 3) où il faut préciser au voisinage de quel point on fait la comparaison.*

Proposition 3.5.1.2 *Dans la pratique, on utilise le critère suivant : si $u_n \neq 0$ pour tout $n \geqslant n_0$, alors :*

$$v_n = O(u_n) \iff \left(\frac{v_n}{u_n}\right)_{n\geqslant n_0} \text{ est bornée}$$

$$v_n = o(u_n) \iff \left(\frac{v_n}{u_n}\right)_{n\geqslant n_0} \text{ converge vers } 0$$

Preuve :

C'est clair car si $u_n \neq 0$ pour tout entier $n \geqslant n_0$, on peut diviser par u_n et on reconnaît la définition de la convergence vers 0 (pour les o) ou d'une suite bornée (pour les O).

⊠

Exercice 3.5.1.3 Que peut-on dire des suites suivantes (en utilisant des O et/ou o) : $\sin(n)$, $n^2 + 3n - 1$, $\ln(n)$, $\frac{\sin n}{n}$?

Exercice 3.5.1.4 Peut-on dire que $\sin(n) = O(2)$? Est-il vrai que $\frac{\ln(1+4n)}{n} = O(1)$?

Corollaire 3.5.1.5 *En particulier, on a :*

$v_n = O(1) \iff (v_n)_{n\in\mathbb{N}}$ *est bornée* et $v_n = o(1) \iff (v_n)_{n\in\mathbb{N}}$ *converge vers* 0

Preuve :

C'est évident. ⊠

Remarques :

- *tout comme pour les fonctions, on notera abusivement* $u_n = O(v_n)$ *(au lieu de* $(u_n) = O((v_n))$*). C'est un abus car les relations o et O sont des relations entre suites, pas entre nombres, mais ceci permet d'alléger les notations et de rendre l'utilisation efficace ;*
- *quand on écrit* $v_n = o(u_n)$ *par exemple, c'est une égalité rigoureuse entre deux suites. La notation* $o(u_n)$ *désigne une suite qui vérifie la propriété d'être négligeable devant* u_n*. Ainsi, on peut écrire :*
$$\frac{n}{1+n} = 1 - \frac{1}{n} + o\left(\frac{1}{n}\right)$$
- *on peut alors faire les calculs usuels, comme avec les développements limités. Par exemple,* $u_n = n + 4 + o(1)$ *et* $v_n = n + o(\sqrt{n})$*, alors :*
$$u_n + v_n = 2n + 4 + o(1) + o(\sqrt{n}) = 2n + o(\sqrt{n})$$
$$u_n v_n = n^2 + 4n + o(n) + o(n\sqrt{n}) + o(4n) + o(1) \times o(n) = n^2 + o(n\sqrt{n})$$
On a utilisé ici qu'une suite (w_n) *qui est* $o(1)$ *est aussi* $o(\sqrt{n})$ *et que si* $(a_n) = o(1)$ *et* $(b_n) = o(n)$*, alors* $(a_n b_n) = o(n)$ *;*
- *pour éviter les erreurs, surtout au début, il vaut mieux écrire tous les termes quand on développe un produit (par exemple) et simplifier seulement à la dernière étape, juste avant de donner une réponse finale ;*
- $(u_n) = o(0)$ *(ou bien* $(u_n) = O(0)$*) si et seulement si la suite* (u_n) *est identiquement nulle à partir d'un certain rang.*

3.5.2 Suites équivalentes

Définition 3.5.2.1 Soient $(u_n)_{n\in\mathbb{N}}$ et $(v_n)_{n\in\mathbb{N}}$ deux suites. On dit que $(u_n)_{n\in\mathbb{N}}$ et $(v_n)_{n\in\mathbb{N}}$ sont équivalentes et on note $(u_n) \sim (v_n)$, ou encore $(u_n) \underset{n\to+\infty}{\sim} (v_n)$, si ces suites vérifient : $(u_n - v_n) = o(v_n)$.

Remarque : *toujours par abus, on note aussi* $u_n \sim v_n$ *ou* $u_n \underset{n\to+\infty}{\sim} v_n$.

Cette définition un peu formelle se traduit dans un cadre pratique de la façon suivante :

Proposition 3.5.2.2 *Soient* $(u_n)_{n\in\mathbb{N}}$ *et* $(v_n)_{n\in\mathbb{N}}$ *deux suites. On suppose que pour tout entier* n *(ou à partir d'un certain rang),* $v_n \neq 0$*. Alors :*

$$u_n \sim v_n \iff \lim_{n\to+\infty} \left(\frac{u_n}{v_n}\right) = 1$$

Preuve :

On suppose qu'il existe un entier n_0 tel que, pour tout $n \geqslant n_0$, $v_n \neq 0$. La suite $(\frac{u_n}{v_n})_{n\geqslant n_0}$ est donc bien définie.

• Montrons l'implication $u_n \sim v_n \Longrightarrow \lim_{n\to+\infty} \left(\frac{u_n}{v_n}\right) = 1$.

On suppose que $u_n \sim v_n$. Montrons que $\lim_{n\to+\infty} \left(\frac{u_n}{v_n}\right) = 1$.

Soit $\varepsilon > 0$. Par définition de l'équivalence $u_n \sim v_n$, il existe un entier N tel que : $\forall n \geqslant N$, $|u_n - v_n| \leqslant \varepsilon |v_n|$. Posons $n_1 = \max(n_0, N)$. On a alors :

$$\forall n \geqslant n_1 \ , \ \left|\frac{u_n}{v_n} - 1\right| \leqslant \varepsilon$$

Ce qui prouve que la suite $(\frac{u_n}{v_n})_{n\geqslant n_0}$ converge vers 1.

• Montrons que $\lim_{n\to+\infty} \left(\frac{u_n}{v_n}\right) = 1 \Longrightarrow u_n \sim v_n$.

On suppose que la suite $(\frac{u_n}{v_n})$ converge vers 1. Soit $\varepsilon > 0$. Il existe un entier $N \in \mathbb{N}$ tel que :

$$\forall n \geqslant \max(N, n_0) \ , \ \left|\frac{u_n}{v_n} - 1\right| \leqslant \varepsilon$$

Or, pour $n \geqslant n_0$, $|v_n| > 0$ donc : $\forall n \geqslant \max(N, n_0)$, $|u_n - v_n| \leqslant \varepsilon |v_n|$.
Ce qui prouve que $u_n \sim v_n$.

⊠

Exemple 3.5.2.3 Les exemples suivants sont usuels et découlent des limites usuelles. Si (u_n) converge vers 0 :

$$\ln(1+u_n) \sim u_n \quad ; \quad \sin(u_n) \sim u_n \quad ; \quad \exp(u_n) - 1 \sim u_n$$

Proposition 3.5.2.4 *La relation $\sim$ est une relation d'équivalence sur l'ensemble des suites, c'est-à-dire qu'elle est réflexive, symétrique et transitive.*
De plus, si $u_n \sim v_n$ alors $u_n = O(v_n)$ et $v_n = O(u_n)$.

Preuve :

• La réflexivité est évidente.

• Montrons que $\sim$ est symétrique.

Soient $(u_n)_{n\in\mathbb{N}}$ et $(v_n)_{n\in\mathbb{N}}$ deux suites telles que $u_n \sim v_n$. Montrons que $v_n \sim u_n$.

Soient $\varepsilon > 0$ et $\varepsilon' = \frac{\varepsilon}{1+\varepsilon}$. Alors $\varepsilon' \in]0,1[$ et $u_n \sim v_n$, donc il existe un entier n_0 tel que :

$$\forall n \geqslant n_0 \ , \ |u_n - v_n| \leqslant \varepsilon' |v_n|$$

Soit $n \geqslant n_0$. On a alors : $|v_n| - |u_n| \leqslant |v_n - u_n| \leqslant \varepsilon' |v_n|$. Par suite, $|v_n| \leqslant \dfrac{|u_n|}{1-\varepsilon'}$.

On en déduit alors que : $|v_n - u_n| \leqslant \varepsilon' |v_n| \leqslant \dfrac{\varepsilon'}{1-\varepsilon'} |u_n| \leqslant \varepsilon |u_n|$.
Ce qui prouve que $v_n \sim u_n$.

• Transitivité
Soient (u_n), (v_n) et (w_n) trois suites telles que : $u_n \sim v_n$ et $v_n \sim w_n$. Soit $\varepsilon > 0$, on pose $\varepsilon' = \frac{\varepsilon}{1+\varepsilon} > 0$. On fixe des entiers n_1 et n_2 tels que :

$$\forall n \geqslant n_1 \ , \ |w_n - v_n| \leqslant \varepsilon' |v_n| \quad \text{et} \quad \forall n \geqslant n_2 \ , \ |v_n - u_n| \leqslant \varepsilon |u_n|$$

Soit $n_0 = \max(n_1, n_2)$ et soit $n \geqslant n_0$. On a alors :

$$|w_n - u_n| \leqslant |w_n - v_n| + |v_n - u_n| \leqslant \varepsilon' |v_n| + \varepsilon |u_n| \leqslant \varepsilon |u_n| + \varepsilon |u_n|$$

c'est-à-dire

$$|w_n - u_n| \leqslant 2\varepsilon |u_n|$$

Par conséquent, $w_n \underset{n\to+\infty}{\sim} u_n$, soit encore $u_n \underset{n\to+\infty}{\sim} w_n$ par symétrie.

⊠

Remarque : *si on suppose que les termes des suites sont tous non nuls à partir d'un certain rang, ces propriétés sont alors toutes évidentes car elles découlent des propriétés algébriques des limites.*

Proposition 3.5.2.5 *Soient $(u_n)_{n\in\mathbb{N}}$ et $(v_n)_{n\in\mathbb{N}}$ deux suites (réelles) équivalentes. Alors à partir d'un certain rang, u_n et v_n sont de même signe strictement. En particulier, $u_n = 0$ si et seulement si $v_n = 0$.*

Preuve :

En effet, soit $\varepsilon = \dfrac{1}{2} > 0$. Par définition de l'équivalence, il existe un entier N tel que :

$$\forall n \geqslant N \ , \ |u_n - v_n| \leqslant \varepsilon |v_n|$$

Alors, pour tout entier $n \geqslant N$, $v_n - \frac{1}{2}|v_n| \leqslant u_n \leqslant v_n + \frac{1}{2}|v_n|$ et :

- si $v_n > 0$, alors $|v_n| = v_n$ et $u_n \geqslant \frac{1}{2}v_n > 0$;
- si $v_n = 0$, alors $u_n = 0$;
- si $v_n < 0$, alors $|v_n| = -v_n$ et $u_n \leqslant \frac{1}{2}v_n < 0$.

⊠

Proposition 3.5.2.6 *On peut multiplier et diviser des équivalents (sauf diviser par 0) mais on ne peut pas toujours les additionner :*

$$\begin{cases} u_n \sim v_n \\ \quad et \\ a_n \sim b_n \end{cases} \Longrightarrow \begin{cases} u_n a_n \sim v_n b_n & \text{(aucune condition)} \\ \dfrac{u_n}{a_n} \sim \dfrac{v_n}{b_n} & \text{(si } a_n \neq 0 \text{ à partir d'un certain rang)} \end{cases}$$

⚠ **Attention :** voici quelques contre-exemples de ce que l'on ne peut pas faire directement. $u_n = n + 1$ et $v_n = -n + 1$ alors $u_n \sim n$ et $v_n \sim -n$ mais $u_n + v_n \sim 2$ et non pas équivalent à 0.

⚠ **Attention :** on ne peut pas composer directement les équivalents. Il faut refaire le travail étape par étape. Par exemple,

$$u_n = n + 1 \quad \text{et} \quad v_n = n \qquad \text{alors } u_n \sim v_n \qquad \text{mais par contre } e^{u_n} \not\sim e^{v_n}$$

Exemple 3.5.2.7 Prenons un exemple simple pour voir les différentes rédaction correctes ou incorrectes. On considère la suite $(u_n) = (\ln\cos(\frac{1}{n}))$ (définie pour $n \geqslant 1$). On veut trouver un équivalent de (u_n).

- Rédaction 1

$$\begin{array}{rll} u_n & \underset{n\to+\infty}{\sim} & \cos(\frac{1}{n})-1 \qquad \text{car} \quad \ln(x) \underset{x\to 1}{\sim} (x-1) \\ & \underset{n\to+\infty}{\sim} & -\frac{1}{2n^2} \qquad\qquad \text{car} \quad \cos(u)-1 \underset{u\to 0}{\sim} -\frac{1}{2}u^2 \end{array}$$

- Rédaction 2

$$\begin{array}{rll} u_n & \underset{n\to+\infty}{\sim} & \ln(1-\frac{1}{2}n^2) \qquad \text{car} \quad \cos(\frac{1}{n}) \underset{n\to+\infty}{\sim} 1-\frac{1}{2n^2} \\ & \underset{n\to+\infty}{\sim} & -\frac{1}{2n^2} \qquad\qquad \text{car} \quad \ln(1-x) \underset{x\to 0}{\sim} -x \end{array}$$

- Rédaction 3

$$\begin{aligned} u_n &= \ln\left(1-\tfrac{1}{2n^2}+o(\tfrac{1}{n^2})\right) \\ &= \left(-\tfrac{1}{2n^2}+o(\tfrac{1}{n^2})\right)+o\left(-\tfrac{1}{2n^2}+o(\tfrac{1}{n^2})\right) \\ &= -\tfrac{1}{2n^2}+o(\tfrac{1}{n^2})+o(\tfrac{1}{n^2}) \\ &\underset{n\to+\infty}{\sim} -\tfrac{1}{2n^2} \end{aligned}$$

On constate que les trois rédactions donnent le même résultat. Cependant,

- les rédactions 1 et 3 sont parfaitement correctes ;
- en revanche, **la rédaction 2 est incorrecte et illogique**. En effet, d'une part on compose des équivalents : $a_n \sim b_n$ n'implique pas $\ln(a_n) \sim \ln(b_n)$! D'autre part, le premier équivalent n'est pas logique car :

$$\cos(\frac{1}{n}) \underset{n\to+\infty}{\sim} 1 \underset{n\to+\infty}{\sim} \left(1-\frac{1}{2n^2}\right) \underset{n\to+\infty}{\sim} \left(1+\frac{1}{n}\right)$$

Il faut donc veiller à bien justifier et rédiger, sans utiliser de composition d'équivalents.

Exemple 3.5.2.8 Soient $u_n = \dfrac{n^2+n+1}{n+1}$ et $v_n = \dfrac{e^{u_n}}{e^n} - 1$. Alors, on a :

$$u_n = n + \frac{1}{n} + o\left(\frac{1}{n}\right) \qquad \text{et} \qquad \frac{e^{u_n}}{e^n} - 1 = \exp\left(\frac{1}{n} + o\left(\frac{1}{n}\right)\right) - 1 = \frac{1}{n} + o\left(\frac{1}{n}\right)$$

Remarque : *on peut prouver, par exemple, les règles de manipulations des o et O suivantes : $O(o(u_n)) = o(u_n)$, si $u_n \sim v_n$ et $(w_n) = o(u_n)$, alors $(w_n) = o(v_n)$.*

Exercice 3.5.2.9 Déterminer la limite puis un équivalent de $\sqrt{n^2+n+1} - \sqrt{n^2+bn+c}$ suivant les valeurs de b et c.

3.5.3 Comparaison des suites de référence

Théorème 3.5.3.1 (Comparaison logarithmique) *Soient (u_n) et (v_n) deux suites réelles à termes strictement positifs (à partir d'un certain rang).*

$$\left(\exists N \in \mathbb{N}\ ,\ \forall n \geqslant N\ ,\ \frac{u_{n+1}}{u_n} \leqslant \frac{v_{n+1}}{v_n}\right) \Longrightarrow u_n = O(v_n)$$

Preuve :

En effet, pour tout n assez grand, $\dfrac{u_{n+1}}{v_{n+1}} \leqslant \dfrac{u_n}{v_n}$: la suite $\left(\dfrac{u_n}{v_n}\right)$ est décroissante (à partir d'un certain rang). Étant minorée par 0, elle est convergente et donc bornée. Par suite, $u_n = O(v_n)$.

⊠

Remarque : *la comparaison logarithmique pour les fonctions revient à comparer $(\ln f)'$ et $(\ln g)'$, c'est-à-dire $\frac{f'}{f}$ et $\frac{g'}{g}$. Pour les suites, c'est $(u_{n+1} - u_n) = (\Delta u_n)$ qui « correspond » à la « dérivée » de (u_n). Le terme $\frac{u_{n+1}}{u_n}$ est donc égal à $\frac{\Delta u_n}{u_n} + 1$. Et on retrouve donc dans les hypothèses du théorème que $\frac{\Delta u_n}{u_n} \leqslant \frac{\Delta v_n}{v_n}$: c'est une des raisons pour lesquelles on parle de comparaison logarithmique.*

Exercice 3.5.3.2 Proposer une autre démonstration qui fait intervenir $(\ln u_n)$ et $(\ln v_n)$ et donner une autre justification du nom "comparaison logarithmique".

Proposition 3.5.3.3 *On a les relations de comparaison suivantes :*

1. *Pour tout $(\alpha, \beta) \in \mathbb{R}^2$ tel que $\alpha < \beta$, $n^\alpha = o(n^\beta)$.*
2. *Pour tout $\alpha \in \mathbb{R}$, pour tout $a > 1$, $n^\alpha = o(a^n)$.*
3. *Pour tout $(a, b) \in \mathbb{R}^2$ tel que $0 < a < b$, $a^n = o(b^n)$.*
4. *Pour tout $\alpha > 0$ et tout $\beta \in \mathbb{R}$, $(\ln n)^\beta = o(n^\alpha)$.*
5. *Pour tout $a > 1$ (et même $a > 0$), $a^n = o(n!)$.*
6. *$n! = o(n^n)$.*

Preuve :

Tout a déjà été prouvé (par calcul direct ou croissances comparées) sauf les propriétés 5 et 6.

• Montrons (5). Soit la suite u de terme général $u_n = \frac{a^n}{n!}$ pour tout entier n. Il est clair que pour tout entier $n \in \mathbb{N}$, $u_n > 0$ et :

$$\forall n \in \mathbb{N}\ ,\ \frac{u_{n+1}}{u_n} = \frac{a}{n+1}$$

On a $\lim\limits_{n\to+\infty} \left(\frac{a}{n+1}\right) = 0$. Par suite, il existe un entier N tel que, $n \geqslant N$ implique $|\frac{a}{n+1}| \leqslant \frac{1}{2}$. Posons alors $v_n = \frac{1}{2^n}$ de sorte que :

$$\forall n \geqslant N\ ,\ \frac{u_{n+1}}{u_n} \leqslant \frac{1}{2} \leqslant \frac{v_{n+1}}{v_n}$$

Les suites $(u_n)_{n\in\mathbb{N}}$ et $(v_n)_{n\in\mathbb{N}}$ étant strictement positives, on a alors d'après le critère de comparaison logarithmique $(u_n) = O(v_n)$. Or, $\lim\limits_{n\to+\infty} v_n = 0$ donc d'après le théorème des gendarmes, $\lim\limits_{n\to+\infty} u_n = 0$, c'est-à-dire $(a^n) = o(n!)$.

• Pour (6), on applique la même méthode : on pose $u_n = \frac{n!}{n^n}$. Vous pouvez montrer que :

$$\lim_{n\to+\infty} \frac{u_{n+1}}{u_n} = \frac{1}{e} < \frac{1}{2}$$

On conclut alors exactement de la même façon que pour 5.

⊠

Remarques : *ce qu'il faut retenir c'est l'échelle de « grandeurs »*

$$(\ln n)^\beta \longrightarrow n^\alpha \longrightarrow a^n \longrightarrow n! \longrightarrow n^n$$

Si les termes sont trop « grands » pour pouvoir les comparer, on calcule les logarithmes (autant de fois que nécessaire) pour pouvoir faire la comparaison.

Exercice 3.5.3.4 On considère les suites (u_n) et (v_n) définies par :

$$\forall n \in \mathbb{N}^\star\ ,\ u_n = 2^{(\ln n)^{\sqrt{n}}} \text{ et } v_n = (\sqrt{n})^{(\ln n)^2}$$

Comparer (au sens de o) les suites (u_n) et (v_n).

3.5.4 Développement asymptotique d'une suite

On ne va pas faire de théorie générale ici. Un développement asymptotique d'une suite est analogue au développement asymptotique d'une fonction. Cela correspond par exemple à utiliser les développements limités pour décrire, avec une précision donnée, le comportement d'une suite.

Exemple 3.5.4.1 Soit $u_n = \sqrt{n+1} - \sqrt{n}$ pour tout entier n. On veut déterminer le comportement de u_n à un $o(\frac{1}{n^2})$ près. On a alors pour tout entier n :

$$\begin{aligned} u_n &= \sqrt{n}\left(\sqrt{1+\frac{1}{n}} - 1\right) \\ &= \sqrt{n}\left(1 + \frac{1}{2n} - \frac{1}{8n^2} + \frac{1}{16n^3} + o(\frac{1}{n^3}) - 1\right) \\ &= \frac{1}{2\sqrt{n}} - \frac{1}{8n\sqrt{n}} + \underbrace{\frac{1}{16n^2\sqrt{n}} + o\left(\frac{1}{n^2\sqrt{n}}\right)}_{o(\frac{1}{n^2})} \\ &= \frac{1}{2\sqrt{n}} - \frac{1}{8n\sqrt{n}} + o\left(\frac{1}{n^2}\right) \end{aligned}$$

On dit qu'on a formé le développement asymptotique de la suite $(u_n)_{n\in\mathbb{N}}$ à $o(\frac{1}{n^2})$ près.

Exemple 3.5.4.2 Montrons que pour tout $n \in \mathbb{N}$, l'équation $x^5 + nx = 1$ admet une unique solution réelle que l'on note x_n puis déterminons le développement asymptotique de (x_n) à 3 termes.

• Soit $n \in \mathbb{N}$. La fonction $f_n : x \longmapsto x^5 + nx$ est continue et strictement croissante sur $\mathbb{R}$. Elle réalise donc une bijection de $\mathbb{R}$ dans $f_n(\mathbb{R}) = \mathbb{R}$. Par suite, l'équation $f_n(x) = 1$ admet une unique solution réelle. On note x_n cette unique solution.

• La question précédente permet donc de définir une suite $(x_n)_{n\in\mathbb{N}}$. On va maintenant former le développement asymptotique à 3 termes. En général, le « plus difficile » est de trouver un équivalent. Une fois l'équivalent trouvé, les termes suivants sont souvent beaucoup plus faciles à obtenir.

∗ Soit $n \in \mathbb{N}^\star$. $f_n(0) = 0 < 1 = f_n(x_n) < 1 + \frac{1}{n^5} = f_n(\frac{1}{n})$. La fonction f_n étant strictement croissante sur $\mathbb{R}$, on obtient :

$$\forall n \in \mathbb{N}^\star\ ,\ 0 < x_n < \frac{1}{n}$$

Or, $\lim\limits_{n\to+\infty} \dfrac{1}{n} = 0$ donc d'après le théorème des gendarmes, $\lim\limits_{n\to+\infty} x_n = 0$.

⚠ **Attention :** cette première étape ne donne pas du tout le premier terme du développement asymptotique ! Ceci permet uniquement de dire que la suite tend vers 0.

Pour tout entier $n \in \mathbb{N}$, $nx_n = 1 - x_n^5$. Or, on vient de montrer que $\lim\limits_{n\to+\infty} x_n = 0$. On en déduit donc que :

$$\lim_{n\to+\infty} nx_n = 1 \quad \text{c'est-à-dire} \quad x_n \underset{n\to+\infty}{\sim} \frac{1}{n}$$

Ce que l'on peut aussi écrire $x_n = \frac{1}{n} + o(\frac{1}{n})$ (et correspond donc au développement asymptotique à 1 terme).

∗ Posons pour $n \in \mathbb{N}^\star$, $y_n = x_n - \frac{1}{n}$. D'après ce qui précède, $(y_n) = o(\frac{1}{n})$. On veut maintenant trouver un équivalent de (y_n). Or, pour $n \in \mathbb{N}^\star$,

$$\left(\frac{1}{n} + y_n\right)^5 + n\left(\frac{1}{n} + y_n\right) = 1$$

c'est-à-dire

$$ny_n = -\left(\frac{1}{n} + y_n\right)^5 = -\frac{1}{n^5}\left(1 + ny_n\right)^5$$

Or, $(y_n) = o(\frac{1}{n})$ donc $\lim\limits_{n\to+\infty} ny_n = 0$ et par suite,

$$\lim_{n\to+\infty} \left(1 + ny_n\right)^5 = 1 \qquad \text{et donc } ny_n \underset{n\to+\infty}{\sim} -\frac{1}{n^5}$$

Ceci montre que $y_n \underset{n\to+\infty}{\sim} -\frac{1}{n^6}$ (le signe est parfaitement en accord avec le début de cette exemple : la suite (y_n) est strictement négative à partir d'un certain rang, c'est-à-dire $x_n < \frac{1}{n}$ à partir d'un certain rang) et donc $x_n = \frac{1}{n} - \frac{1}{n^6} + o\left(\frac{1}{n^6}\right)$ (on a donc obtenu le développement asymptotique de (x_n) à deux termes).

∗ Posons enfin pour $n \in \mathbb{N}^\star$, $z_n = y_n + \frac{1}{n^6}$. Par hypothèse, $(z_n) = o(\frac{1}{n^6})$ et pour tout entier $n \geqslant 1$:

$$n\left(-\frac{1}{n^6} + z_n\right) = -\frac{1}{n^5}\left(1 + n\left(-\frac{1}{n^6} + z_n\right)\right)^5$$

soit encore,

$$\begin{aligned} nz_n &= -\frac{1}{n^5}\left[\left(1 - \frac{1}{n^5} + nz_n\right)^5 - 1\right] \\ &= -\frac{1}{n^5}\left[\left(1 - \frac{1}{n^5} + o(\frac{1}{n^5}\right)^5 - 1\right] \\ &= -\frac{1}{n^5}\left(1 - \frac{5}{n^5} + o(\frac{1}{n^5}) - 1\right) \\ &\underset{n\to+\infty}{\sim} \frac{5}{n^{10}} \end{aligned}$$

Ce qui montre que $z_n \underset{n\to+\infty}{\sim} \frac{5}{n^{11}}$ et donc finalement :

$$x_n = \frac{1}{n} - \frac{1}{n^6} + \frac{5}{n^{11}} + o\left(\frac{1}{n^{11}}\right)$$

Exercice 3.5.4.3 On considère la fonction f définie sur $\mathcal{D}_f = \mathbb{R} \setminus \{\frac{\pi}{2} + n\pi \ , \ n \in \mathbb{Z}\}$ par la relation :

$$\forall x \in \mathcal{D}_f \ , \ f(x) = \tan(x) - x$$

1. Montrer que pour chaque entier $n \in \mathbb{N}$, la restriction de la fonction f à l'intervalle $I_n =]-\frac{\pi}{2} + n\pi, \frac{\pi}{2} + n\pi[$ réalise une bijection de I_n dans $\mathbb{R}$.
2. En déduire que pour tout entier $n \in \mathbb{N}$, il existe un unique réel $x_n \in I_n$ tel que $\tan(x_n) = x_n$.
3. Déterminer un équivalent de x_n.
4. Déterminer le développement asymptotique de $(x_n)_{n\in\mathbb{N}}$ à trois termes.

Exercice 3.5.4.4 On considère la suite $(u_n)_{n\in\mathbb{N}}$ définie par $u_0 > 0$ et la relation de récurrence :

$$\forall n \in \mathbb{N} \ , \ u_{n+1} = \ln(1 + u_n)$$

1. Prouver que la suite $(u_n)_{n\in\mathbb{N}}$ converge vers 0.
2. Pour $\alpha \in \mathbb{R}$, déterminer un équivalent de $u_{n+1}^\alpha - u_n^\alpha$ (en fonction de α et u_n uniquement).
3. En déduire qu'il existe une unique valeur de α (que vous déterminerez) telle que la suite $(u_{n+1}^\alpha - u_n^\alpha)$ converge vers une limite $\ell \neq 0$.
4. En utilisant le théorème de Césaro [5], déterminer alors un équivalent de (u_n).

3.6 Suites à valeurs complexes

3.6.1 Définitions et convergence d'une suite complexe

Définition 3.6.1.1 Une suite à valeurs complexes est une application $u : \mathbb{N} \longrightarrow \mathbb{C}$, ou de façon équivalente, une famille de nombres complexes indexée par $\mathbb{N}$.

Définition 3.6.1.2 Soit $(z_n)_{n\in\mathbb{N}}$ une suite complexe. On définit alors les suites :

$$(u_n) = \Re e(z_n) = (\Re e(z_n))_{n\in\mathbb{N}} \quad ; \quad (v_n) = \Im m(z_n) = (\Im m(z_n))_{n\in\mathbb{N}}$$

$$\text{et} \quad \overline{(z_n)_{n\in\mathbb{N}}} = (\overline{z}_n)_{n\in\mathbb{N}}$$

5. voir l'exercice à la fin de ce chapitre.

On remarque alors qu'on peut étendre toutes les définitions ne faisant pas intervenir la relation d'ordre de $\mathbb{R}$ aux cas des suites complexes.

Par exemple, il n'y a aucun sens à parler de suite complexe croissante ou majorée... En revanche, la distance dans $\mathbb{R}$ est remplacée par le module dans $\mathbb{C}$. On peut donc définir une suite complexe bornée : une suite complexe $(z_n)_{n\in\mathbb{N}}$ est bornée s'il existe un réel $M \geqslant 0$ tel que : $\forall n \in \mathbb{N}, |z_n| \leqslant M$.

Définition 3.6.1.3 On dit qu'une suite complexe $(z_n)_{n\in\mathbb{N}}$ converge vers $\ell \in \mathbb{C}$ si :

$$\forall \varepsilon > 0 \ , \ \exists N \in \mathbb{N} \ , \ \forall n \geqslant N \ , \ |z_n - \ell| \leqslant \varepsilon$$

Si une suite $(z_n)_{n\in\mathbb{N}}$ converge vers $\ell \in \mathbb{C}$, alors ℓ est unique et est appelé la limite de la suite.

Les propriétés suivantes restent valables pour les suites complexes :

1. Toute suite convergente est bornée.
2. Toute suite extraite d'une suite convergente est convergente et sa limite est la même que la suite de départ.
3. La somme et le produit de deux suites convergentes est convergente et on a les mêmes règles de calculs des limites.
4. Le quotient de deux suites convergentes dont le dénominateur converge vers un complexe non nul, est une suite convergente et la limite est le quotient des limites.
5. Le théorème de Bolzano-Weierstrass reste valable pour une suite complexe.
6. Les notions de suites équivalentes, dominées et négligeables, ainsi que leurs propriétés restent valables.

En revanche, les propriétés suivantes n'ont aucun sens pour les suites complexes :

1. Une suite complexe monotone.
2. Une suite complexe majorée (ou minorée).
3. Le théorème des gendarmes et le théorème de la limite monotone.
4. Le théorème des suites adjacentes.
5. Les conclusions sur les signes.

3.6.2 Lien avec les parties réelle et imaginaire

Théorème 3.6.2.1 *Une suite complexe $(z_n)_{n\in\mathbb{N}}$ converge vers $\ell \in \mathbb{C}$ si et seulement si $\Re e(z_n)$ converge vers $\Re e(\ell)$ et $\Im m(z_n)$ converge vers $\Im m(\ell)$.*

Preuve :

Ceci découle des limites des fonctions à valeurs vectorielles (voir par exemple les calculs de limites pour les courbes paramétrées) après avoir identifié $\mathbb{C}$ au plan $\mathbb{R}^2$. Rappelons néanmoins l'idée principale.
Si on note pour $n \in \mathbb{N}$, $z_n = x_n + iy_n$ avec $(x_n, y_n) \in \mathbb{R}^2$ et $\ell = a + ib$ avec $(a, b) \in \mathbb{R}^2$, alors :

$$\forall n \in \mathbb{N}\ ,\ \max(|x_n - a|, |y_n - b|) \leqslant |z_n - \ell| \leqslant \sqrt{2}\max(|x_n - a|, |y_n - b|)$$

On retrouve immédiatement que :

$$\lim_{n\to+\infty} |z_n - \ell| = 0 \iff \left(\lim_{n\to+\infty} |x_n - a| = 0 \text{ et } \lim_{n\to+\infty} |y_n - b| = 0\right)$$

⊠

Exercice 3.6.2.2 Étudier la suite (z_n) définie par $z_{n+1} = \dfrac{1+i}{2} z_n$ et $z_0 \in \mathbb{C}$.

Exercice 3.6.2.3 Étudier la suite $(z_n)_{n\in\mathbb{N}}$ définie par $z_n = \dfrac{n^2 + 3n - 1}{-3n^2 + 4} + i\dfrac{n!}{n^n}$.

Exercice 3.6.2.4 Déterminer un équivalent de la suite $(z_n)_{n\in\mathbb{N}}$ définie par :

$$\forall n \in \mathbb{N}\ ,\ z_n = \frac{\arctan(n) + ie^{-n}}{n^2 + in + 1}$$

3.7 Exercices

Exercice 3.7.1 Soit $(x_n)_{n\in\mathbb{N}}$ une suite réelle telle que (x_{2n}), (x_{2n+1}) et (x_{3n}) convergent. Montrer que $(x_n)_{n\in\mathbb{N}}$ converge.

Exercice 3.7.2 Montrer que les suites $(\cos(n))_{n\in\mathbb{N}}$ et $(\sin(n))_{n\in\mathbb{N}}$ divergent.

Exercice 3.7.3 Soit $(u_n)_{n\in\mathbb{N}}$ une suite à valeurs dans $\mathbb{Z}$. Montrer que $(u_n)_{n\in\mathbb{N}}$ converge si et seulement si $(u_n)_{n\in\mathbb{N}}$ est stationnaire, c'est-à-dire que $(u_n)_{n\in\mathbb{N}}$ est constante à partir d'un certain rang.

Exercice 3.7.4 Soit (u_n) une suite de réels strictement positifs. On suppose que la suite $(\frac{u_{n+1}}{u_n})$ admet une limite et on note $\lim\limits_{n\to+\infty} \dfrac{u_{n+1}}{u_n} = \ell \in [0,+\infty]$.

1. Montrer que si $\ell < 1$, alors $\lim\limits_{n\to+\infty} u_n = 0$ puis montrer que si $\ell > 1$, alors $\lim\limits_{n\to+\infty} u_n = +\infty$.
2. Que peut-on dire si $\ell = 1$?

Exercice 3.7.5 Soit $(u_n)_{n\in\mathbb{N}}$ une suite de réels non majorée. Démontrer qu'il existe une suite extraite de $(u_n)_{n\in\mathbb{N}}$ tendant vers $+\infty$.

Exercice 3.7.6 Soit $(u_n)_{n\in\mathbb{N}}$ une suite réelle telle que :

$$\forall (m,n) \in (\mathbb{N}^*)^2,\ \ 0 \leq u_{m+n} \leq \frac{m+n}{mn}$$

Montrer que (u_n) converge vers 0.

Exercice 3.7.7 (Théorème de Césaro) Soit $(u_n)_{n\in\mathbb{N}}$ une suite réelle. On suppose que $\lim\limits_{n\to+\infty} u_n = \ell \in \overline{\mathbb{R}}$. Montrer que :

$$\lim_{n\to+\infty} \frac{1}{n+1} \sum_{k=0}^{n} u_k = \ell$$

Montrer que le résultat reste vrai pour une suite complexe qui converge vers $\ell \in \mathbb{C}$.

Exercice 3.7.8 Les affirmations suivantes sont-elles vraies ou fausses ? On justifiera les réponses par une preuve ou un contre-exemple :

1. « Si (u_n) est une suite telle que (u_n^2) converge, alors la suite (u_n) converge ».
2. « Si (u_n) est à termes positifs et (u_n^2) converge, alors la suite (u_n) converge ».
3. « Si (u_n) est une suite telle que (u_n^2) et (u_n^3) convergent, alors (u_n) converge ».
4. « Soient (a_n) une suite bornée et (ε_n) une suite convergeant vers 0. Alors la suite de terme général $u_n = \varepsilon_n a_n$ converge vers 0 ».
5. « Soient (a_n) une suite bornée et (ε_n) une suite qui converge. Alors la suite de terme général $u_n = \varepsilon_n a_n$ converge ».
6. « Soient (a_n) une suite majorée et (ε_n) une suite non majorée. Alors la suite de terme général $u_n = \varepsilon_n a_n$ n'est pas majorée ».
7. « Si (u_n) converge, alors $(u_{n+1} - u_n)$ converge vers 0 ».
8. « Si $(u_{n+1} - u_n)$ converge vers 0, alors (u_n) converge ».
9. « Si $u_n \sim v_n$ alors $(u_n - v_n)$ converge vers 0 ».
10. « Si $(u_n - v_n)$ converge vers 0, alors $u_n \sim v_n$ ».
11. « Si (u_n) et (v_n) convergent et si $u_n \leqslant w_n \leqslant v_n$ alors(w_n) converge ».
12. « Si (u_n) est une suite de réels strictement positifs qui converge vers 0, alors (u_n) est décroissante à partir d'un certain rang ».

Exercice 3.7.9 Montrer que pour tout entier n, $(3+\sqrt{5})^n + (3-\sqrt{5})^n \in 2\mathbb{Z}$. En déduire que la suite $\left(\sin\left((3+\sqrt{5})^n \pi\right)\right)$ converge.

Exercice 3.7.10 Étudier la convergence de la suite $(u_n)_{n\in\mathbb{N}}$ définie par $u_0 = u_1 = 1$ et pour tout entier n, $u_{n+2} = -u_{n+1} - \dfrac{1}{4}u_n$.

Exercice 3.7.11 Étudier la suite définie par $u_0 = 1$, $u_1 = 2$ et pour tout entier $n \in \mathbb{N}$, $u_{n+2} = \sqrt{u_n u_{n+1}}$.

Exercice 3.7.12 Étudier la convergence, suivant les valeurs de u_0 et de $k \in \mathbb{C}$, de la suite $(u_n)_{n\in\mathbb{N}}$ vérifiant $\forall n \in \mathbb{N}$, $u_{n+1} - u_n = k^n$.

Exercice 3.7.13 On considère la suite $(u_n)_{n\in\mathbb{N}}$ définie par $u_0 = \frac{3}{2}$ et pour tout entier n, $u_{n+1} = u_n^2 - 2u_n + 2$.

1. Démontrer par récurrence que pour tout entier n, $1 \leqslant u_n \leqslant 2$. *On pourra étudier les variations de $f : x \mapsto x^2 - 2x + 2$.*
2. Étudier les variations de $(u_n)_{n\in\mathbb{N}}$. Que peut-on en déduire ?
3. Déterminer la limite de $(u_n)_{n\in\mathbb{N}}$.

Exercice 3.7.14 Étudier, suivant les valeurs du réel a, la suite (u_n) définie par $u_0 = a$ et $\forall n \in \mathbb{N}$, $u_{n+1} = u_n^2 + \dfrac{3}{16}$.

Exercice 3.7.15 Soit $a > 0$. On considère la suite $(u_n)_{n\in\mathbb{N}}$ définie par $u_0 > 0$ et la relation de récurrence : $\forall n \in \mathbb{N}$, $u_{n+1} = \dfrac{1}{2}\left(u_n + \dfrac{a}{u_n}\right)$.

1. Étudier la convergence de la suite $(u_n)_{n\in\mathbb{N}}$. Préciser sa limite si elle converge.
2. On pose pour tout entier n, $v_n = \dfrac{u_n - \sqrt{a}}{u_n + \sqrt{a}}$.
   (a) Exprimer, pour $n \in \mathbb{N}$, v_{n+1} en fonction de v_n.
   (b) En déduire que si $u_0 > \sqrt{a}$, alors pour tout entier n, $|u_n - \sqrt{a}| < 2u_0 v_0^{2^n}$.
   (c) Application : déterminer une fraction rationnelle approchant $\sqrt{2}$ à 10^{-11} près.

Exercice 3.7.16 Soit $(u_n)_{n\in\mathbb{N}}$ définie par $u_0 = 1$ et $\forall n \in \mathbb{N}$, $u_{n+1} = \dfrac{u_n + 2u_n^2}{1 + 3u_n}$.

1. Démontrer que $\forall n \in \mathbb{N}$, $u_n > 0$.
2. Montrer que $(u_n)_{n\in\mathbb{N}}$ converge et déterminer sa limite ℓ.
3. On veut maintenant déterminer un équivalent de $u_n - \ell$.
   (a) Montrer que $\dfrac{1}{1+3u_n} = 1 - 3u_n + o(u_n)$ puis que $u_{n+1} = u_n - u_n^2 + o(u_n^2)$.
   (b) On fixe $\alpha \in \mathbb{R}^\star$. Montrer que : $u_{n+1}^\alpha - u_n^\alpha \underset{n\to+\infty}{\sim} -\alpha u_n^{\alpha+1}$.
   (c) Quelle valeur de α faut-il choisir pour obtenir un équivalent simple ? Justifier la réponse.
   (d) On suppose par la suite que $\alpha = -1$. Montrer que $u_n \underset{n\to+\infty}{\sim} \dfrac{1}{n}$.

   Indication : on pourra utiliser sans démonstration le théorème de Césaro (voir exercice 3.7.7) et reconnaître une série télescopique.

Exercice 3.7.17 On considère la suite définie par $u_0 = 1$ et $\forall n \in \mathbb{N}$, $u_{n+1} = \dfrac{u_n}{u_n^2 + 1}$.

1. Montrer que $(u_n)_{n\in\mathbb{N}}$ converge et déterminer sa limite.
2. Montrer que la suite $(u_{n+1}^{-2} - u_n^{-2})$ converge vers 2.
3. En utilisant le théorème de Césaro (exercice 3.7.7), déterminer un équivalent de $(u_n)_{n\in\mathbb{N}}$.

Exercice 3.7.18 On considère la suite $(x_n)_{n\in\mathbb{N}}$ définie par $x_0 > 0$ et pour tout entier n, $x_{n+1} = x_n + \dfrac{1}{x_n^2}$.

1. Montrer que la suite $(x_n)_{n\in\mathbb{N}}$ est bien définie.
2. Étudier la suite $(x_n)_{n\in\mathbb{N}}$ et montrer que $(x_n)_{n\in\mathbb{N}}$ admet une limite que vous déterminerez.
3. Montrer qu'il existe $\alpha \in \mathbb{R}$ que vous déterminerez tel que $x_{n+1}^\alpha - x_n^\alpha \underset{n\to+\infty}{\sim} 3$.
4. En déduire un équivalent de x_n.

Exercice 3.7.19 On pose pour $n \in \mathbb{N}$, $u_n = \displaystyle\int_0^1 (1-t)^n e^t \,\mathrm{d}t$.

1. Calculer u_0, u_1 et u_2.
2. Étudier les variations de la suite $(u_n)_{n\in\mathbb{N}}$ et prouver que $(u_n)_{n\in\mathbb{N}}$ converge.
3. Montrer que pour tout entier n, $0 \leqslant u_n \leqslant \dfrac{e}{n+1}$. En déduire la limite de la suite $(u_n)_{n\in\mathbb{N}}$.
4. Établir que pour tout $n \in \mathbb{N}$, $u_{n+1} = (n+1)u_n - 1$.
5. À l'aide d'un tableur ou de Matlab, calculer les 15 premiers termes de la suite $(u_n)_{n\in\mathbb{N}}$ en utilisant $u_0 = e - 1$ et la relation de récurrence. Que constate-t-on ? Comment expliquer cela ?
6. On considère à présent l'ensemble $\mathcal{S}$ des suites réelles $(v_n)_{n\in\mathbb{N}}$ vérifiant la relation de récurrence :
$$\forall n \in \mathbb{N}\ ,\ v_{n+1} = (n+1)v_n - 1$$
   (a) $\mathcal{S}$ est-il un groupe pour la loi $+$? Est-il un sous-anneau de l'ensemble des suites ? Est-il un sous-espace vectoriel des suites ?
   (b) Soit $(v_n)_{n\in\mathbb{N}} \in \mathcal{S}$. Montrer que : $\forall n \in \mathbb{N}\ ,\ v_{n+1} - u_{n+1} = (n+1)(v_n - u_n)$.
   (c) En déduire l'expression de v_n en fonction de n, u_n et v_0.
   (d) En déduire une condition nécessaire et suffisante pour qu'une suite $(v_n)_{n\in\mathbb{N}} \in \mathcal{S}$ converge.

Exercice 3.7.20 On considère les suites $(u_n)_{n\in\mathbb{N}}$ et $(v_n)_{n\in\mathbb{N}}$ définies par $u_0 = 1$, $v_0 = 1$ et la relation de récurrence :
$$\forall n \in \mathbb{N}\ ,\ \left\{\begin{array}{rcl} u_{n+1} &=& 6u_n + 5v_n \\ v_{n+1} &=& -3u_n - 2v_n \end{array}\right.$$
Démontrer que $(u_n)_{n\in\mathbb{N}}$ et $(v_n)_{n\in\mathbb{N}}$ vérifient une relation de récurrence linéaire d'ordre deux, à coefficients constants et en déduire les expressions de u_n et v_n en fonction de n uniquement.

Exercice 3.7.21 On pose pour tout entier non nul n, $S_n = \sum_{k=1}^{n} \frac{(-1)^k}{k}$.

1. Montrer que les suites (S_{2n}) et (S_{2n+1}) sont adjacentes. La suite $(S_n)_{n\in\mathbb{N}}$ est-elle convergente ?
2. Soient $x \in [0,1]$ et $n \in \mathbb{N}^\star$.
   (a) Montrer que $\forall t \in [0,x]$, $\frac{1}{1+t} = \sum_{k=0}^{n} (-1)^k t^k + (-1)^{n+1} \frac{t^{n+1}}{1+t}$.
   (b) En déduire que pour $x \in [0,1]$, $\ln(1+x) = \sum_{k=0}^{n} \frac{(-1)^k}{k+1} x^{k+1} + (-1)^{n+1} \int_0^x \frac{t^{n+1}}{1+t}\,\mathrm{d}t$ et conclure que $\ln 2 = \lim_{n\to+\infty} \sum_{k=0}^{n} \frac{(-1)^k}{k+1}$.
   (c) Que peut-on en déduire pour $(S_n)_{n\in\mathbb{N}}$?

Exercice 3.7.22 Soit (S_n) définie par pour tout entier $n \geqslant 1$, $S_n = \sum_{k=1}^{n} \frac{(-1)^k}{k^3}$.

1. Démontrer que les suites (S_{2n}) et (S_{2n+1}) sont adjacentes.
2. En déduire que (S_n) converge et déterminer une valeur approchée par défaut à 10^{-2} près.

Exercice 3.7.23 On considère les suites définies par :

$$u_0 = 1 \quad v_0 = 2 \quad \text{et} \quad \forall n \in \mathbb{N}\ ,\ \frac{2}{u_{n+1}} = \frac{1}{u_n} + \frac{1}{v_n} \quad \text{et} \quad v_{n+1} = \frac{u_n + v_n}{2}$$

1. Montrer que les suites $(u_n)_{n\in\mathbb{N}}$ et $(v_n)_{n\in\mathbb{N}}$ sont des suites de rationnels.
2. Montrer que les deux suites convergent vers la même limite et déterminer la valeur de la limite.

Exercice 3.7.24 On considère les suites $(u_n)_{n\in\mathbb{N}}$ et $(v_n)_{n\in\mathbb{N}}$ définies par :

$$0 < u_0 < v_0 \quad \text{et} \quad \forall n \in \mathbb{N}\ ,\ u_{n+1} = \frac{u_n^2}{u_n + v_n} \ \text{ et } \ v_{n+1} = \frac{v_n^2}{u_n + v_n}$$

Montrer que les deux suites sont bien définies et étudier la convergence de ces deux suites.

Exercice 3.7.25 Soient $0 < a < b$ et les suites (u_n) et (v_n) définies par : $u_0 = a$, $v_0 = b$ et pour tout entier n,

$$u_{n+1} = \frac{u_n + v_n}{2} \quad \text{et} \quad v_{n+1} = \sqrt{u_{n+1} v_n}$$

Montrer que les suites (u_n) et (v_n) convergent vers une même limite que l'on exprimera à l'aide du réel $\alpha \in]0,\pi[$ défini par la relation $b\cos\alpha = a$.

Exercice 3.7.26 À l'aide d'une comparaison avec une intégrale, démontrer que la suite définie pour $n \geqslant 2$ par : $S_n = \sum_{k=2}^{n} \frac{1}{k\sqrt{\ln k}}$ diverge vers $+\infty$ et déterminer un équivalent de S_n.

Exercice 3.7.27 Déterminer la nature de la série $\sum E(\ln n)$, puis déterminer un équivalent des sommes partielles.

Exercice 3.7.28 On considère la suite (S_n) définie pour tout entier non nul n par :

$$S_n = \sum_{k=1}^{n} \frac{1}{k}$$

1. Étudier la nature de la suite (S_n).
2. À l'aide d'une comparaison avec une intégrale, donner un équivalent de S_n.
3. On pose pour $n \in \mathbb{N}^\star$, $u_n = S_n - \ln n$.
   (a) Étudier les variations de (u_n).
   (b) Montrer que la suite (u_n) converge et que sa limite γ est un réel de l'intervalle $[0, 1]$.
4. De façon analogue, on définit la suite $v_n = S_{n-1} - \ln n$ pour $n \geqslant 2$ et $v_1 = 0$.
   (a) Par un raisonnement analogue, prouver que (v_n) converge.
   (b) En déduire que une valeur approchée de γ à 10^{-1} près.
5. Quel développement asymptotique les résultats précédents permettent-ils de mettre en évidence ?

Exercice 3.7.29 Soit (u_n) une suite à termes positifs telle que : $\forall n \geqslant 1, u_n + u_{2n} = \frac{3}{2n}$.

1. Montrer que (u_n) converge vers 0.
2. Soit $n \geqslant 1$. On pose pour tout entier k, $v_k = u_{2^k n} + u_{2^{k+1} n}$.
   (a) Exprimer, pour $k \in \mathbb{N}$, v_k en fonction de n et k uniquement.
   (b) Pour tout $N \in \mathbb{N}$, exprimer $u_n - u_{2^{2N+2} n}$ en fonction des v_k pour $k \in \mathbb{N}$.
   (c) En déduire que $\forall n \in \mathbb{N}^\star$, $u_n = \frac{1}{n}$.

Exercice 3.7.30 Utiliser des équivalents simples pour calculer les limites suivantes :

$$\lim_{n\to+\infty}\left(1+\frac{x}{n}\right)^n \;;\; \lim_{n\to+\infty}\left(\frac{n-1}{n+1}\right)^n \;;\; \lim_{n\to+\infty}\left(\frac{n}{n-x}\right)^n \;;\; \lim_{n\to+\infty}\left(\frac{n^2+3n+1}{n^2-2n+1}\right)^n$$

où pour la première suite, on suppose que $x \in \mathbb{R}$.

Exercice 3.7.31 Déterminer un équivalent simple pour chacune des suites suivantes :

$$u_n = \sqrt{n+1}-\sqrt{n-1} \;;\; v_n = \frac{1}{n-2}-\frac{1}{n+1} \;;\; w_n = n\sin\left(\frac{1}{\sqrt{n}}\right) \;;\; x_n = n^{\frac{1}{n}}-1$$

$$y_n = \ln(n+1)-\ln(n) \quad ; \quad z_n = \tan\left(\frac{\pi}{4}+\frac{1}{n}\right) \quad ; \quad s_n = \left(\tan\left(\frac{\pi}{4}+\frac{1}{n}\right)\right)^n$$

Exercice 3.7.32 Déterminer les limites éventuelles des suites suivantes :

1. $u_n = \sqrt{n^2+n+1}-\sqrt{n^2-n+1}$ et $v_n = \sqrt{n+\sqrt{n^2+1}}-\sqrt{n+\sqrt{n^2-1}}$
2. $w_n = \dfrac{n-\sqrt{n^2+1}}{n-\sqrt{n^2-1}}$ et $a_n = \dfrac{E\left((n+\frac{1}{2})^2\right)}{E\left((n-\frac{1}{4})^2\right)}$
3. $b_n = n^{\frac{1}{\ln n}}$ et $c_n = (\ln n)^{\frac{1}{n}}$
4. $d_n = n^{\frac{\sin n}{n}}$ et $e_n = \left(\sin\left(\frac{1}{n}\right)\right)^{\frac{1}{\ln n}}$
5. $f_n = \dfrac{1}{n^2}\displaystyle\sum_{k=1}^{n} E(kx)$ où $x \in \mathbb{R}$ et E désigne la partie entière.

Exercice 3.7.33 Montrer que $\displaystyle\sum_{k=1}^{n} k! \leqslant n \times n!$ et en déduire que $\displaystyle\sum_{k=1}^{n} k! \sim n!$.

Exercice 3.7.34 Soient $(u_n)_{n\in\mathbb{N}}$ et $(v_n)_{n\in\mathbb{N}}$ deux suites réelles qui convergent vers 0. Montrer que $(e^{u_n}-e^{v_n}) \underset{n\to+\infty}{\sim} (u_n-v_n)$. Le résultat est-il encore vrai si les deux suites sont complexes et tendent vers 0 ?

Exercice 3.7.35 Soient $(\alpha_n)_{n\in\mathbb{N}} \in \mathbb{C}^{\mathbb{N}}$, $(\beta_n)_{n\in\mathbb{N}} \in \mathbb{C}^{\mathbb{N}}$ et $(u_n)_{n\in\mathbb{N}} \in \mathbb{R}^{\mathbb{N}}$.

1. On suppose que $\alpha_n \underset{n\to+\infty}{\sim} \beta_n$ et que pour tout $n \in \mathbb{N}$, $\Re e(\alpha_n) \neq 0$ et $\Re e(\beta_n) \neq 0$. A-t-on $\Re e(\alpha_n) \underset{n\to+\infty}{\sim} \Re e(\beta_n)$?
2. On suppose que $u_{n+1} \underset{n\to+\infty}{\sim} u_n$. A-t-on $u_{2n} \underset{n\to+\infty}{\sim} u_n$?
3. Soit ℓ un réel. On suppose que $u_n \underset{n\to+\infty}{\sim} \ell$. A-t-on $u_n^n \underset{n\to+\infty}{\sim} \ell^n$?

Exercice 3.7.36 Pour $n \in \mathbb{N}^\star$, on considère la fonction $P_n : x \longmapsto x^n + x^{n-1} + \cdots + x - 1$.

1. Montrer que le polynôme P_n admet une unique racine positive. On la note x_n.
2. Montrer que pour tout $n \in \mathbb{N}^\star$, $P_n(x_{n+1}) < 0$. En déduire les variations de $(x_n)_{n\in\mathbb{N}}$.
3. Montrer que $(x_n)_{n\in\mathbb{N}}$ converge et déterminer sa limite ℓ.
4. Déterminer un équivalent de $x_n - \ell$. *On pourra poser $y_n = x_n - \ell$ et commencer par montrer que $y_n = O(x_2^n)$.*

Exercice 3.7.37

1. Montrer que pour tout entier $n \in \mathbb{N}$, l'équation $x + 3\ln x = n$ admet une unique solution. On note x_n cette solution.
2. Déterminer la limite de la suite (x_n).
3. Déterminer un équivalent simple de (x_n).
4. Montrer qu'il existe a, b, c trois réels non nuls (que vous déterminerez) tels que :

$$x_n = an + b\ln n + c\frac{\ln n}{n} + o\left(\frac{\ln n}{n}\right)$$

Exercice 3.7.38

1. Montrer que pour tout entier $n \in \mathbb{N}^\star$, le polynôme $P_n = X^n + X - 1$ admet une unique racine dans $]0, 1[$.
2. On note pour $n \in \mathbb{N}^\star$, x_n l'unique racine de P_n dans $]0, 1[$.
   (a) Montrer que (x_n) converge et déterminer sa limite ℓ.
   (b) On cherche à déterminer un équivalent de $x_n - \ell$. On pose $x_n = \ell - y_n$.
      (i) Montrer que : $-\dfrac{\ln y_n}{y_n} \underset{n\to+\infty}{\sim} n$.
      (ii) Prouver alors que $\ln y_n \underset{n\to+\infty}{\sim} -\ln n$ et en déduire un équivalent de y_n.

Exercice 3.7.39 Soit $z = x + iy$, avec $(x, y) \in \mathbb{R}^2$. Démontrer que $\lim\limits_{n\to+\infty} \left(1 + \dfrac{z}{n}\right)^n = e^z$.

Exercice 3.7.40 Soit $(z_n)_{n\in\mathbb{N}}$ définie par $z_0 \in \mathbb{C}$ et $\forall n \in \mathbb{N}$, $z_{n+1} = \frac{1}{2}(z_n + |z_n|)$. La suite $(z_n)_{n\in\mathbb{N}}$ est-elle convergente ? Si oui, déterminer sa limite.

Exercice 3.7.41 (Difficile) Soit $u = (u_n)_{n\in\mathbb{N}}$ une suite réelle. On dit que $\ell \in \mathbb{R}$ est **valeur d'adhérence** de la suite u s'il existe une suite extraite de $(u_n)_{n\in\mathbb{N}}$ de limite ℓ.

1. On suppose u bornée. L'ensemble de ses valeurs d'adhérence peut-il être vide ?
2. On suppose que u est bornée et que la suite $(u_{n+1} - u_n)_{n\in\mathbb{N}}$ converge vers 0. Montrer que l'ensemble des valeurs d'adhérence de u est un segment.
3. Donner un exemple de suite réelle dont l'ensemble des valeurs d'adhérence est $\mathbb{R}$.

Exercice 3.7.42 On note $\mathcal{S}$ l'ensemble des suites réelles vérifiant la relation de récurrence :

$$\forall n \geqslant 1 \ , \ u_{n+1} = (4n+2)u_n + u_{n-1}$$

Partie 1 : structure de $\mathcal{S}$

1. Montrer que $(\mathcal{S}, +)$ est un groupe abélien et que $\mathcal{S}$ est stable par multiplication externe. *Autrement dit, montrer que $(\mathcal{S}, +, \cdot)$ est un $\mathbb{R}$-espace-vectoriel.*
2. Montrer que l'application $\phi : \begin{array}{ccc} \mathcal{S} & \longrightarrow & \mathbb{R}^2 \\ (u_n) & \longmapsto & (u_0, u_1) \end{array}$ est un isomorphisme de $(\mathcal{S}, +)$ sur $(\mathbb{R}^2, +)$.
3. Montrer de plus que ϕ préserve la multiplication externe.

Partie 2 : étude de la convergence

1. Soit $(u_n) \in \mathcal{S}$. On suppose que $(u_n)_{n\in\mathbb{N}}$ converge. Que peut-on dire de sa limite ?
2. Soient $(a_n)_{n\in\mathbb{N}} \in \mathcal{S}$ et $(b_n)_{n\in\mathbb{N}} \in \mathcal{S}$ vérifiant : $a_0 = b_1 = 1$ et $a_1 = b_0 = 0$.
   (a) Démontrer que (b_n) est croissante et que $\forall n \geqslant 1$, $b_n \geqslant 6^{n-1}$. Que peut-on en déduire ?
   (b) On définit la suite (w_n) par $w_n = a_n b_{n+1} - a_{n+1} b_n$. Montrer que (w_n) est géométrique et en déduire l'expression de w_n en fonction de n uniquement.
   (c) On considère enfin la suite (t_n) définie pour tout $n \geqslant 1$ par $t_n = \dfrac{a_n}{b_n}$.
      (i) Montrer que les suites (t_{2n}) et (t_{2n+1}) convergent vers la même limite ℓ que l'on ne cherchera pas à calculer.
      (ii) Que peut-on en déduire sur la suite (t_n) ?
3. On veut à présent déterminer une condition nécessaire et suffisante portant sur u_0 et u_1 pour qu'une suite (u_n) de $\mathcal{S}$ converge.
   (a) On suppose que $(u_n) \in \mathcal{S}$ converge.
      (i) Montrer que $\forall n \in \mathbb{N}$, $u_n = u_0 a_n + u_1 b_n$.
      (ii) En déduire que $u_0 \ell + u_1 = 0$.
   (b) Réciproquement, on suppose que $u_0 \ell + u_1 = 0$.
      (i) Montrer que pour tout entier $n \geqslant 1$, $\left| \ell - \dfrac{a_n}{b_n} \right| \leqslant \dfrac{1}{b_n b_{n+1}}$.
      (ii) En déduire que $(a_n - \ell b_n)$ converge et déterminer sa limite.
      (iii) Conclure.

Exercice 3.7.43 Pour un calcul célèbre, Archimède considéra les relations de récurrence suivantes :

$$c_{n+1} = \sqrt{\frac{1+c_n}{2}} \quad \text{et} \quad \lambda_{n+1} = \frac{\lambda_n}{c_{n+1}}$$

1. Rappeler brièvement qui était Archimède, l'époque à laquelle il a vécu ainsi que les principaux résultats qu'il a découvert en sciences.
2. Montrer que pour $c_1 = 0$ et $\lambda_1 = 2$, ces relations définissent deux suites $(c_n)_{n\geqslant 1}$ et $(\lambda_n)_{n\geqslant 1}$ et qu'il existe deux autres suites $(\theta_n)_{n\geqslant 1}$ et $(\alpha_n)_{n\geqslant 1}$ telles que :
$$\forall n \in \mathbb{N}^\star\ ,\ \theta_n \in \left]0;\frac{\pi}{2}\right]\ \ ,\ \ \alpha_n > 0\ \ ,\ \ c_n = \cos(\theta_n)\ \ ,\ \ \lambda_n = \alpha_n \sin(\theta_n)$$
3. Étude de la suite $(\lambda_n)_{n\geqslant 1}$
   (a) Montrer que la suite (λ_n) converge vers π.
   (b) En utilisant que pour tout $x \geqslant 0$, $|\sin x - x| \leqslant \dfrac{x^3}{6}$, montrer que pour tout $n \geqslant 1$, $|\lambda_n - \pi| \leqslant \dfrac{\pi^3}{6\times 4^n}$.
   (c) Déterminer un entier n_1 tel que $|\lambda_{n_1} - \pi| \leqslant 10^{-6}$.
4. On définit une nouvelle suite $(\lambda'_n)_{n\geqslant 1}$ par $\lambda'_n = \dfrac{4\lambda_{n+1} - \lambda_n}{3}$.
   (a) Établir que (λ'_n) converge aussi vers π.
   (b) Montrer que $\lambda'_n - \pi = o\left(\dfrac{1}{4^n}\right)$ et en déduire que $\lambda'_n - \pi = o(\lambda_n - \pi)$. *On pourra utiliser le développement limité à l'ordre* 3 *en* 0 *de la fonction sinus.*
   (c) Comment peut-on interpréter concrètement par une phrase le résultat de la question précédente.
   (d) En utilisant le développement limité à l'ordre 5 en 0 de sinus, déterminer un équivalent de $\lambda'_n - \pi$.
5. Pour $\alpha \in \mathbb{R}$, on définit une nouvelle suite (λ''_n) par $\lambda''_n = \alpha\lambda'_n + (1-\alpha)\lambda'_{n+1}$.
   (a) Montrer qu'il existe un unique $\alpha \in \mathbb{R}$ tel que $\lambda''_n - \pi = o\left(\dfrac{1}{4^{2n}}\right)$.
   (b) Pour cette valeur de α, exprimer λ''_n en fonction de λ_n, λ_{n+1} et λ_{n+2}.
   (c) On admet que pour tout entier $n \geqslant 1$, il existe $x_n \in]0, \theta_n[$ tel que :
   $$\lambda_n = \pi - \frac{\pi^3}{3!}\times\frac{1}{4^n} + \frac{\pi^5}{5!}\times\frac{1}{4^{2n}} - \frac{\pi^7}{7!}\times\frac{1}{4^{3n}}\cos(x_n)$$
   Montrer alors que pour tout $n \geqslant 1$, $|\lambda''_n - \pi| \leqslant \dfrac{17\pi^7}{576\times 7!}\times\dfrac{1}{4^{3n}}$.
   (d) Déterminer un entier n_2 tel que l'on ait $|\lambda''_n - \pi| \leqslant 10^{-6}$.
6. Quel commentaire peut-on faire ?

Chapitre 4

Espaces vectoriels et applications linéaires

Prérequis : dans tout ce chapitre, les notions suivantes sont supposées connues :

- le cours de logique (en particulier, implications et équivalences) ;
- notion d'ensemble et opérations usuelles sur les ensembles (intersection, union et produit cartésien) ;
- image directe et image réciproque d'une partie par une application ;
- structures usuelles : groupes, anneaux et corps ;
- morphisme de groupes ;
- injection, surjection, bijection et leurs propriétés.

4.1 Espaces vectoriels

Dans tout ce chapitre, la lettre $\mathbb{K}$ désigne un corps commutatif. Dans la pratique $\mathbb{K} = \mathbb{R}$ ou $\mathbb{K} = \mathbb{C}$.

4.1.1 Définition et exemples usuels

Définition 4.1.1.1 Soient E un ensemble et $\mathbb{K}$ un corps commutatif (ici $\mathbb{K} = \mathbb{R}$ ou $\mathbb{K} = \mathbb{C}$). On dit que E est un espace vectoriel sur $\mathbb{K}$ (ou bien un $\mathbb{K}$-espace vectoriel) lorsque E est muni :

- d'une loi de composition interne, notée $+$, telle que $(E, +)$ soit un groupe abélien ;
- d'une loi de composition externe $\mathbb{K} \times E \longrightarrow E$, , notée $\cdot$, vérifiant les propriétés suivantes :

  P1 $\forall (\lambda, \mu) \in \mathbb{K}^2$, $\forall u \in E$, $(\lambda + \mu) \cdot u = \lambda \cdot u + \mu \cdot u$

  P2 $\forall \lambda \in \mathbb{K}$, $\forall (u, v) \in E^2$, $\lambda \cdot (u + v) = \lambda \cdot u + \lambda \cdot v$

  P3 $\forall (\lambda, \mu) \in \mathbb{K}^2$, $\forall u \in E$, $(\lambda \times \mu) \cdot u = \lambda \cdot (\mu \cdot u)$

  P4 $\forall u \in E$, $1_{\mathbb{K}} \cdot u = u$

Les éléments de E sont appelés les vecteurs et les éléments de $\mathbb{K}$ les scalaires.

Exemple 4.1.1.2 L'ensemble des vecteurs du plan (ou de l'espace) est un $\mathbb{R}$-espace vectoriel : c'est d'ailleurs ce qu'on a pris comme modèle pour définir la notion d'espace vectoriel.

Remarque : *ainsi, normalement, on doit préciser que $(E, +, \cdot)$ est un $\mathbb{K}$-espace vectoriel (c'est-à-dire préciser les lois de compositions interne et externe). Dans la pratique, comme pour les groupes ou les anneaux, on dira simplement « soit E un $\mathbb{K}$-espace vectoriel ».*

Proposition 4.1.1.3 *Soit $n \in \mathbb{N}^\star$. On munit l'ensemble $\mathbb{K}^n$ de deux opérations : on pose pour $\lambda \in \mathbb{K}$ et $u, v \in \mathbb{K}^n$ avec $u = (u_1, \cdots, u_n)$ et $v = (v_1, \cdots, v_n)$,*

$$u + v = (u_1 + v_1, \cdots, u_n + v_n) \qquad et \qquad \lambda \cdot u = (\lambda \times u_1, \cdots, \lambda \times u_n)$$

Alors $(\mathbb{K}^n, +, \cdot)$ est un $\mathbb{K}$-espace vectoriel.

Preuve :

• On a déjà montré que $(\mathbb{K}^n, +)$ est un groupe commutatif (voir la proposition 1.1.2.5).

• L'opération $\cdot$ est une application bien définie de $\mathbb{K} \times \mathbb{K}^n$ dans $\mathbb{K}^n$.

∗ Montrons $P1$.
Soient $u = (u_k)_{1 \leqslant k \leqslant n} \in \mathbb{K}^n$ et $(\lambda, \mu) \in \mathbb{K}^2$. On a alors :

$$\begin{aligned}(\lambda + \mu) \cdot u &= ((\lambda + \mu) \times u_1, \cdots, (\lambda + \mu) \times u_n) \text{ (par définition de } \cdot) \\ &= (\lambda \times u_1 + \mu \times u_1, \cdots, \lambda \times u_n + \mu \times v_n)\end{aligned}$$

car $\times$ est distributive par rapport à l'addition dans $\mathbb{K}$. Alors, par définition de $+$ dans $\mathbb{K}^n$,

$$\begin{aligned}(\lambda + \mu) \cdot u &= (\lambda \times u_1, \cdots, \lambda \times u_n) + (\mu \times u_1, \cdots, \mu \times u_n) \\ &= \lambda \cdot u + \mu \cdot u\end{aligned}$$

∗ Montrons $P2$.
Soient $u = (u_l, \cdots, u_n)$ et $v = (v_1, \cdots, v_n)$ deux éléments de $\mathbb{K}^n$ et $\lambda \in \mathbb{K}$. Alors :

$$\begin{aligned}\lambda \cdot (u + v) &= \lambda \cdot (u_1 + v_1, \cdots, u_n + v_n) \\ &= (\lambda \times (u_1 + v_1), \cdots, \lambda \times (u_n + v_n)) \\ &= (\lambda \times u_1 + \lambda \times v_1, \cdots, \lambda \times u_n + \lambda \times v_n) \\ &= (\lambda \times u_1, \cdots, \lambda \times u_n) + (\lambda \times v_1, \cdots, \lambda \times v_n) \\ &= \lambda \cdot u + \lambda \cdot v\end{aligned}$$

∗ Montrons $P3$.
Soient $u = (u_1, \cdots, u_n) \in \mathbb{K}^n$ et $\lambda, \mu \in \mathbb{K}$. On a :

$$\begin{aligned}\lambda \cdot (\mu \cdot u) &= \lambda \cdot (\mu \times u_1, \cdots, \mu \times u_n) \\ &= (\lambda \times (\mu \times u_1), \cdots, \lambda \times (\mu \times u_n)) \\ &= ((\lambda \times \mu) \times u_1, \cdots, (\lambda \times \mu) \times u_n) \quad (\times \text{ est associative sur } \mathbb{K}) \\ &= (\lambda \times \mu) \cdot (u_1, \cdots, u_n) \\ &= (\lambda \times \mu) \cdot u\end{aligned}$$

∗ Montrons $P4$.
Puisque $1_{\mathbb{K}}$ est neutre pour la multiplication dans $\mathbb{K}$, il est clair que pour tout $u = (u_1, \cdots, u_n) \in \mathbb{K}^n$:

$$1_{\mathbb{K}} \cdot u = (1_{\mathbb{K}} \times u_1, \cdots 1_{\mathbb{K}} \times u_n) = (u_1, \cdots, u_n) = u$$

Ce qui prouve que $(\mathbb{K}^n, +, \cdot)$ est bien un $\mathbb{K}$-espace vectoriel. ⊠

Remarques :

- *en particulier,* $\mathbb{K}$ *est un* $\mathbb{K}$*-espace vectoriel (correspond à* $n = 1$*) ;*
- $\mathbb{C}$ *est donc un* $\mathbb{C}$*-espace vectoriel mais est aussi un* $\mathbb{R}$*-espace vectoriel ! Ces deux espaces vectoriels ne sont pas les mêmes. Il est donc important de bien préciser s'il s'agit d'un* $\mathbb{R}$*-espace vectoriel ou bien d'un* $\mathbb{C}$*-espace vectoriel.*

En fait, on a un résultat un peu plus général : c'est l'objet de la proposition suivante.

Proposition 4.1.1.4 *Soit* X *un ensemble quelconque et* F *un* $\mathbb{K}$*-espace vectoriel. Alors l'ensemble* $\mathcal{F}(X, F)$ *est un* $\mathbb{K}$*-espace vectoriel pour les opérations suivantes définies pour tout* $f, g \in \mathcal{F}(X, F)$ *et* $\lambda \in \mathbb{K}$ *:*

$$\begin{array}{rcl} f+g : X & \longrightarrow & F \\ x & \longmapsto & f(x)+g(x) \end{array} \quad \textit{et} \quad \begin{array}{rcl} \lambda \cdot f : X & \longrightarrow & F \\ x & \longmapsto & \lambda \cdot f(x) \end{array}$$

⚠ **Attention :** notez bien qu'il y a deux opérations $+$ et $\cdot$: celles qu'on définit sur l'ensemble $\mathcal{F}(X, F)$ et celles de F qui sont données. On les note de la même façon pour ne pas alourdir les notations mais en toute rigueur, on devrait écrire : $(F, +, \cdot)$ et $(\mathcal{F}(X, F), \oplus, \odot)$. Avec ces notations, on a pour tout $x \in X$, $(f \oplus g)(x) = f(x) + g(x)$ et $(\lambda \odot f)(x) = \lambda \cdot f(x)$. Par la suite, on ne fera jamais cette distinction et on notera seulement $+$ et $\cdot$ mais faites bien attention à ne pas les confondre.

Preuve :

La démonstration est identique à la précédente. Voici les étapes essentielles de la démonstration :

- Pour montrer que $(\mathcal{F}(X, F), +)$ est un groupe :
  - c'est toujours un ensemble non vide puisque F est non vide ;
  - $+$ est associative et commutative car l'addition dans F est associative et commutative ;
  - l'application nulle (c'est-à-dire constante égale à 0_F) est clairement neutre pour $+$;
  - si $f \in \mathcal{F}(X, F)$, alors l'application $g \in \mathcal{F}(X, F)$ définie par : $\forall x \in X$, $g(x) = -f(x)$ est l'opposé de f pour la loi $+$.
- Les propriétés $P1$, $P2$, $P3$ et $P4$ pour $\mathcal{F}(X, F)$ sont des conséquences directes de ces mêmes propriétés pour $(F, +, \cdot)$.

Les détails de la preuve sont laissés en exercice.

⊠

Corollaire 4.1.1.5 *Soit I un intervalle réel (ou une partie quelconque de $\mathbb{R}$ ou $\mathbb{C}$). Les ensembles $\mathbb{R}^{\mathbb{N}}$, $\mathbb{R}^{\mathbb{R}}$ et $\mathcal{F}(I,\mathbb{R})$ sont des $\mathbb{R}$-espaces vectoriels. $\mathbb{C}^{\mathbb{N}}$, $\mathbb{C}^{\mathbb{R}}$ et $\mathcal{F}(I,\mathbb{C})$ sont des $\mathbb{C}$-espaces vectoriels.*

Remarque : *il est important de bien connaître les espaces vectoriels de référence. On verra un peu plus loin que comme pour les groupes ou les anneaux, pour montrer que E est un espace vectoriel, on montrera très souvent que c'est un sous-espace vectoriel d'un espace vectoriel de référence.*

⚠ **Attention :** on a vu dans le chapitre sur les groupes et anneaux que $(\mathbb{Z}^n,+,\times)$ (avec l'addition et la multiplication terme à terme) est un anneau. En revanche, $\mathbb{Z}^n$ n'est pas un $\mathbb{R}$-espace vectoriel ! $\mathbb{Z}^n$ n'est pas non plus un $\mathbb{Z}$-espace vectoriel car $\mathbb{Z}$ n'est pas un corps et donc la notion de $\mathbb{Z}$-espace vectoriel n'est pas définie.

Exercice 4.1.1.6 On munit $\mathbb{Z}$ de l'addition usuelle. Montrer qu'il n'existe pas de loi de composition externe $\cdot$ de $\mathbb{R}\times\mathbb{Z}$ dans $\mathbb{Z}$ telle que $(\mathbb{Z},+,\cdot)$ soit un $\mathbb{R}$-espace vectoriel.

4.1.2 Règles de calcul dans un espace vectoriel

Essentiellement, on retrouve presque toutes les mêmes règles de calcul que dans un anneau.

Proposition 4.1.2.1 *Soit $(E,+,\cdot)$ un $\mathbb{K}$-espace vectoriel. Alors :*

(i) « La loi $\cdot$ est distributive par rapport aux lois $+$ ». De façon plus formelle, on a pour tout $(n,p)\in\mathbb{N}^2$, $(\lambda,\lambda_0,\cdots,\lambda_p)\in\mathbb{K}^{p+1}$ et $(u,u_0,\cdots,u_n)\in E^{n+1}$:

$$\lambda\cdot\left(\sum_{i=0}^{n}u_i\right)=\sum_{i=0}^{n}(\lambda\cdot u_i)\qquad et\qquad\left(\sum_{k=0}^{p}\lambda_k\right)\cdot u=\sum_{k=0}^{p}(\lambda_k\cdot u)$$

(ii) $\forall u\in E\ ,\ 0_{\mathbb{K}}\cdot u=0_E$

(iii) $\forall\lambda\in\mathbb{K}\ ,\ \lambda\cdot 0_E=0_E$

(iv) $\forall(\lambda,u)\in\mathbb{K}\times E\ ,\ \lambda\cdot u=0_E\iff\lambda=0_{\mathbb{K}}\ ou\ u=0_E$

(v) $\forall u\in E\ ,\ -u=(-1)\cdot u$

(vi) « Distributivité de $\cdot$ par rapport à $-$ » :

$$\forall(\lambda,\mu)\in\mathbb{K}^2\ ,\ \forall(u,v)\in E^2\ ,\ (\lambda-\mu)\cdot u=\lambda\cdot u-\mu\cdot u\ \ et\ \ \lambda\cdot(u-v)=\lambda\cdot u-\lambda\cdot v$$

Preuve :

• (i) est une conséquence directe de la définition d'un espace vectoriel et se prouve rigoureusement par récurrence sur n (respectivement p). Exercice : rédiger cette récurrence.

• Montrons (ii).
On copie la preuve dans le cas des anneaux :

$$0_{\mathbb{K}} \cdot u = (0_{\mathbb{K}} + 0_{\mathbb{K}}) \cdot u = 0_{\mathbb{K}} \cdot u + 0_{\mathbb{K}} \cdot u$$

Dans le groupe $(E, +)$ tout élément admet un opposé : par conséquent, $0_{\mathbb{K}} \cdot u = 0_E$.

• La démonstration de (iii) est identique à la précédente en calculant $\lambda \cdot (0_E + 0_E)$.

• Montrons (iv).
On peut remarquer que $\Longleftarrow$ vient d'être démontrée (il s'agit de (ii) et (iii)). Réciproquement, on constate que :

$$\Big(\lambda \cdot u = 0_E \Longrightarrow \lambda = 0_{\mathbb{K}} \text{ ou } u = 0_E\Big) \iff \Big(\lambda \cdot u = 0_E \text{ et } \lambda \neq 0_{\mathbb{K}} \Longrightarrow u = 0_E\Big)$$

Soient λ un scalaire non nul et u un vecteur de E tels que $\lambda \cdot u = 0_E$. $\mathbb{K}$ est un corps et $\lambda \neq 0_{\mathbb{K}}$ donc λ admet un inverse pour la loi $\times$ dans $\mathbb{K}$. Il vient alors :

$$0_E = \lambda^{-1} \cdot 0_E = \lambda^{-1} \cdot (\lambda \cdot u) = (\lambda^{-1} \times \lambda) \cdot u = 1_{\mathbb{K}} \cdot u = u$$

• Montrons (v). Soit $u \in E$. Alors :

$$u + (-1_{\mathbb{K}}) \cdot u = 1_{\mathbb{K}} \cdot u + (-1_{\mathbb{K}}) \cdot u = (1_{\mathbb{K}} + (-1_{\mathbb{K}})) \cdot u = 0_{\mathbb{K}} \cdot u = 0_E$$

Or, $+$ est commutative (dans E) donc $(-1_{\mathbb{K}}) \cdot u + u = u + (-1_{\mathbb{K}}) \cdot u = 0_E$, ce qui prouve que $-u = (-1_{\mathbb{K}}) \cdot u$.

• La propriété (vi) est une conséquence directe de (v) et des propriétés P1, P2 et P3. La preuve rigoureuse est laissée en exercice. ⊠

⚠ **Attention :** notez la différence fondamentale dans les règles entre espaces vectoriels et anneaux :

dans un espace vectoriel, $\quad \lambda \cdot u = 0 \iff \lambda = 0$ ou $u = 0$

dans un anneau, $\quad a \times b = 0 \not\Longrightarrow a = 0$ ou $b = 0$

Remarque : *quels sont les anneaux A pour lesquels $a \times b = 0 \Longrightarrow a = 0$ ou $b = 0$ est vraie pour tout $(a, b) \in A^2$?*

Définition 4.1.2.2 Soient $n \in \mathbb{N}^\star$, E un $\mathbb{K}$-espace vectoriel et $(u_1, \cdots, u_n) \in E^n$. On appelle combinaison linéaire des vecteurs $u_1, \cdots, u_n$ tout vecteur $v \in E$ s'écrivant sous la forme :

$$v = \sum_{k=1}^{n} \lambda_k \cdot u_k$$

où $\lambda_1, \cdots, \lambda_n$ sont des scalaires, c'est-à-dire pour tout $k \in [\![1, n]\!]$, $\lambda_k \in \mathbb{K}$.

Exemple 4.1.2.3 Dans l'espace habituel muni de sa base $(\vec{i}, \vec{j}, \vec{k})$, un vecteur $\vec{v}$ est combinaison linéaire de $\vec{i}$ et $\vec{j}$ s'il s'écrit sous la forme :

$$\vec{u} = \lambda\vec{i} + \mu\vec{j} \quad \text{avec } (\lambda, \mu) \in \mathbb{R}^2$$

On peut alors remarquer que l'ensemble de toutes les combinaisons linéaires de $\vec{i}$ et $\vec{j}$ est le plan de base $(\vec{i}, \vec{j})$. C'est ce qu'on appelle le sous-espace vectoriel engendré par $\vec{i}$ et $\vec{j}$. On reverra cela un peu plus loin.

Exemple 4.1.2.4 Soit $E = \mathcal{F}(\mathbb{R}, \mathbb{R})$. On a vu que c'est un $\mathbb{R}$-espace vectoriel. Pour $n \in \mathbb{N}$ donné, si on pose pour $k \in [\![0, n]\!]$, $f_k : x \longmapsto x^k$, alors $f_k \in E$ et une fonction f est combinaison linéaire des vecteurs $(f_k)_{0 \leqslant k \leqslant n}$ si et seulement si elle s'écrit sous la forme :

$$f = \sum_{k=0}^{n} \lambda_k f_k \text{ avec } (\lambda_k)_{0 \leqslant k \leqslant n} \in \mathbb{R}^{n+1} \text{ soit encore } \forall x \in \mathbb{R}\ ,\ f(x) = \sum_{k=0}^{n} \lambda_k x^k$$

C'est-à-dire que f est combinaison linéaire des vecteurs $(f_k)_{0 \leqslant k \leqslant n}$ si et seulement si f est une fonction polynomiale de degré au plus n.

Exemple 4.1.2.5 On considère $E = \mathbb{R}^{\mathbb{N}}$ (qui est bien un $\mathbb{R}$-espace vectoriel) et on note $\mathcal{S} = \{(u_n) \in E \ / \ \forall n \in \mathbb{N}\ ,\ u_{n+2} - 5u_{n+1} + 10u_n = 0\}$. Soit $(u_n)_{n\in\mathbb{N}} \in \mathbb{R}^{\mathbb{N}}$. Alors on a vu que $(u_n)_{n\in\mathbb{N}} \in \mathcal{S}$ si et seulement si $(u_n)_{n\in\mathbb{N}}$ est combinaison linéaire de $(2^n)_{n\in\mathbb{N}}$ et $(5^n)_{n\in\mathbb{N}}$.

4.1.3 Sous-espaces vectoriels

Définition 4.1.3.1 Soient E un $\mathbb{K}$-espace vectoriel et $F \subset E$. On dit que F est un sous-$\mathbb{K}$-espace vectoriel de E (ou simplement sous-espace vectoriel de E) si :

(i) $0_E \in F$;

(ii) F est stable par $+$, c'est-à-dire : $\forall (u, v) \in F^2\ ,\ u + v \in F$;

(iii) F est stable par $\cdot$, c'est-à-dire : $\forall \lambda \in \mathbb{K}\ ,\ \forall u \in F\ ,\ \lambda \cdot u \in F$.

Remarques :

- *les propriétés (ii) et (iii) sont équivalentes à :*

$$(ii)\ bis : \quad \forall(\lambda,\mu)\in\mathbb{K}^2\ ,\ \forall(u,v)\in F^2\ ,\ \lambda\cdot u+\mu\cdot v\in F$$

  ou encore au fait que F est stable par combinaisons linéaires. En effet, si (ii) bis est vérifiée, alors en choisissant $\lambda=\mu=1_{\mathbb{K}}$, on obtient (ii). Puis en choisissant $\mu=0$, on obtient (iii). Réciproquement, si (ii) et (iii) sont vérifiées, alors pour $(u,v)\in F^2$ et $(\lambda,\mu)\in\mathbb{K}^2$, on a $\lambda\cdot u\in F$ et $\mu\cdot v\in F$ d'après (iii), et donc $\lambda\cdot u+\mu\cdot v\in F$ d'après (ii).
- *par abus (mais c'est une notation utilisée par tous), on notera E est un $\mathbb{K}$-ev (pour dire que E est un $\mathbb{K}$-espace vectoriel) et F est un sev de E, au lieu de F est un sous-espace vectoriel de E.*

Proposition 4.1.3.2 *Soient E un $\mathbb{K}$-espace vectoriel et F un sous-espace vectoriel de E. Alors $(F,+,\cdot)$ est un $\mathbb{K}$-espace vectoriel.*

Preuve :

• Tout d'abord, montrons que $(F,+)$ est un sous-groupe de $(E,+)$.

  ∗ par définition $F\subset E$ et d'après (i), $0_E\in F$;

  ∗ d'après (ii), F est stable par $+$;

  ∗ montrons que F est stable par opposé. Soit $u\in F$, alors d'après (iii), $(-1)\cdot u\in F$. Mais dans E, qui est un espace vectoriel, $(-1)\cdot u=-u$: par suite, $-u\in F$.

Ce qui montre que $(F,+)$ est un sous-groupe de $(E,+)$ donc est bien un groupe.

• La loi $\cdot$ est bien une loi de composition externe : $\mathbb{K}\times F\longrightarrow F$ d'après (iii).

• Les propriétés $P1$, $P2$, $P3$ et $P4$ étant vraies sur E, elles le sont *a fortiori* sur F. ⊠

▶ Méthode :

Pour montrer que F est un espace vectoriel, on montre souvent que c'est un sous-espace vectoriel d'un espace vectoriel E connu. Pour cela, on utilise généralement la caractérisation suivante :

$$(i) : \quad 0_E\in F$$
$$(ii) : \quad \forall(\lambda,\mu)\in\mathbb{K}^2\ ,\ \forall(u,v)\in F^2\ ,\ \lambda\cdot u+\mu\cdot v\in F$$

Exemple 4.1.3.3 Si I est un intervalle non vide de $\mathbb{R}$, l'ensemble $\mathcal{C}^0(I,\mathbb{C})$ des fonctions continues sur I à valeurs complexes est un $\mathbb{C}$-espace vectoriel, c'est un sous-espace vectoriel de $\mathcal{F}(I,\mathbb{C})$. En effet,

- la fonction nulle est continue sur I donc $0_{\mathcal{F}(I,\mathbb{C})} \in \mathcal{C}^0(I,\mathbb{C})$;
- si $f,g \in \mathcal{C}^0(I,\mathbb{C})$ et $\lambda,\mu \in \mathbb{C}$, alors $\lambda f + \mu g$ est aussi continue sur I (puisque f et g le sont), c'est-à-dire $\lambda f + \mu g \in \mathcal{C}^0(I,\mathbb{C})$.

Exemple 4.1.3.4 L'ensemble des suites convergentes est un sous-espace vectoriel des suites bornées, lui-même étant un sous-espace vectoriel de $\mathbb{R}^{\mathbb{N}}$. En effet,

- $\mathcal{B}(\mathbb{N},\mathbb{R}) \subset \mathbb{R}^N$;
- la suite nulle est bornée donc $0_{\mathbb{R}^{\mathbb{N}}} \in \mathcal{B}(\mathbb{N},\mathbb{R})$;
- on a prouvé dans le chapitre précédent, que si u,v sont des suites bornées et $\lambda \in \mathbb{R}$ alors $u+v$ et $\lambda \cdot u$ sont bornées, c'est-à-dire que $\mathcal{B}(\mathbb{N},\mathbb{R})$ est stable par combinaisons linéaires.

Ce qui prouve que $\mathcal{B}(\mathbb{N},\mathbb{R})$ est bien un sous-espace vectoriel de $\mathbb{R}^{\mathbb{N}}$.

De la même façon, en notant $\mathcal{S}$ l'ensemble des suites réelles convergentes, on a montré que :

- $\mathcal{S} \subset \mathcal{B}(\mathbb{N},\mathbb{R})$ (toute suite convergente est bornée) ;
- la suite nulle converge donc $0_{\mathcal{B}(\mathbb{N},\mathbb{R})} \in \mathcal{S}$;
- si $u=(u_n)_{n\in\mathbb{N}}$ et $v=(v_n)_{n\in\mathbb{N}}$ sont deux suites convergentes et si λ,μ sont deux réels, alors $\lambda \cdot u + \mu \cdot v$ converge, c'est-à-dire $\lambda \cdot u + \mu \cdot v \in \mathcal{S}$.

Ce qui prouve que $\mathcal{S}$ est bien un sous-espace vectoriel de $\mathcal{B}(\mathbb{N},\mathbb{R})$.

Exemple 4.1.3.5 Notons $E=\mathcal{C}^0([0,1],\mathbb{R})$ et $F=\{f\in E \ / \ \int_0^1 f(x)\,\mathrm{d}x = 0\}$. Montrons que F est un sous-espace vectoriel de E.

- $F \subset E$ par définition ;
- la fonction nulle sur $[0,1]$ est d'intégrale nulle sur $[0,1]$ donc $0_E \in F$;
- soient $(f,g)\in F^2$ et $(\lambda,\mu)\in\mathbb{R}^2$. La fonction $\lambda f+\mu g$ (qui est bien continue sur $[0,1]$ car E est un espace vectoriel) vérifie par « linéarité » de l'intégrale :

$$\int_0^1 (\lambda f+\mu g)(x)\,\mathrm{d}x = \int_0^1 (\lambda f(x)+\mu g(x))\,\mathrm{d}x = \lambda\int_0^1 f(x)\,\mathrm{d}x + \mu\int_0^1 g(x)\,\mathrm{d}x = 0$$

  c'est-à-dire $\lambda f+\mu g \in F$.

Ce qui prouve que F est bien un sous-espace vectoriel de E.

Remarque : *on verra un peu plus loin une méthode plus rapide pour justifier que F est un sous-espace vectoriel de E (et même un hyperplan) : c'est le noyau d'une application linéaire.*

Exercice 4.1.3.6 Montrer que l'ensemble des solutions de $y'' + y = 0$ est un sous-espace vectoriel de $\mathcal{C}^0(\mathbb{R}, \mathbb{R})$.

Exemple 4.1.3.7 Soit $E = \mathbb{R}^3$. On note $(u|v)$ le produit scalaire des deux vecteurs u et v dans $\mathbb{R}^3$. On rappelle que si $u = (x, y, z)$ et $v = (x', y', z')$, alors $(u|v) = xx' + yy' + zz'$. Soit u est un vecteur de $\mathbb{R}^3$. Montrons que l'ensemble $u^\perp = \{v \in \mathbb{R}^3 \ / \ (u|v) = 0\}$ (l'ensemble des vecteurs orthogonaux à u, c'est-à-dire l'ensemble des vecteurs dont le produit scalaire usuel avec u est nul) est un espace vectoriel.

- Tout d'abord, $u^\perp \subset \mathbb{R}^3$;
- ensuite, $(u|0) = 0$ donc $0_{\mathbb{R}^3} \in u^\perp$;
- enfin, soient $(v_1, v_2) \in (u^\perp)^2$ et $(\lambda, \mu) \in \mathbb{R}^2$. Alors, d'après les propriétés du produit scalaire [1] :

$$(u|\lambda v_1 + \mu v_2) = \lambda(u|v_1) + \mu(u|v_2) = \lambda \times 0_{\mathbb{R}} + \mu \times 0_{\mathbb{R}} = 0$$

et donc $\lambda v_1 + \mu v_2 \in u^\perp$.

Exemple 4.1.3.8 En revanche, les ensembles $F = \{f \in \mathcal{C}^0([0,1], \mathbb{R}) \ / \ \displaystyle\int_0^1 f(x)\,\mathrm{d}x = 1\}$ et $\mathcal{P} = \{(x, y, z) \in \mathbb{R}^3 \ / \ x + y + z = 1\}$ ne sont pas des espaces vectoriels. L'ensemble $\mathcal{P}$ est un plan « affine » mais n'est pas un plan « vectoriel ».

Exercice 4.1.3.9 L'ensemble $F = \{(u_n)_{n\in\mathbb{N}} \in \mathbb{R}^{\mathbb{N}} \ / \ (u_n^2)_{n\in\mathbb{N}} \text{ converge }\}$ est-il un sous-espace vectoriel de $\mathbb{R}^{\mathbb{N}}$?

Exercice 4.1.3.10 L'ensemble $\mathcal{B} = \{(x, y) \in \mathbb{R}^2 \ / \ x^2 + y^2 < 1\}$ est-il un sous-espace vectoriel de $\mathbb{R}^2$? Est-il stable par addition ? Est-il stable par multiplication externe ?

Définition 4.1.3.11 Soient E un espace vectoriel et u un vecteur non nul. On pose alors :

$$\mathbb{K} \cdot u = \{\lambda \cdot u \ , \ \lambda \in \mathbb{K}\}$$

On dit que $\mathbb{K} \cdot u$ est la droite vectorielle dirigée par u ou que u est un vecteur directeur de $\mathbb{K} \cdot u$.

Proposition 4.1.3.12 *Soit $u \in E \setminus \{0_E\}$. Alors, $\mathbb{K} \cdot u$ est un sous-espace vectoriel de E. De plus, tout élément non nul de $\mathbb{K} \cdot u$ est un vecteur directeur de $\mathbb{K} \cdot u$.*

1. le produit scalaire « usuel » est bilinéaire donc linéaire à droite.

Preuve :

• Montrons pour commencer que $\mathbb{K}u$ est un sous-espace vectoriel de E.

∗ En prenant $\lambda = 0$, on a $0_{\mathbb{K}} \cdot u \in \{\lambda \cdot u \ , \ \lambda \in \mathbb{K}\}$, c'est-à-dire $0_E \in \mathbb{K}u$.

∗ Soient $(\lambda, \mu) \in \mathbb{K}^2$ et $(v, w) \in (\mathbb{K}u)^2$. Par définition, il existe $\lambda_1 \in \mathbb{K}$ et $\lambda_2 \in \mathbb{K}$ tels que : $v = \lambda_1 \cdot u$ et $w = \lambda_2 \cdot u$. On a alors :

$$\begin{aligned} \lambda \cdot v + \mu \cdot w &= \lambda \cdot (\lambda_1 \cdot u) + \mu \cdot (\lambda_2 \cdot u) \\ &= (\lambda \times \lambda_1) \cdot u + (\mu \times \lambda_2) \cdot u \\ &= (\lambda \times \lambda_1 + \mu \times \lambda_2) \cdot u \end{aligned}$$

Or, $(\lambda \times \lambda_1 + \mu \times \lambda_2) \in \mathbb{K}$ donc $\lambda \cdot v + \mu \cdot v \in \mathbb{K}u$.

Ce qui prouve que $\mathbb{K}u$ est bien un sous-espace vectoriel de E.

• Montrons à présent que tout vecteur non nul de $\mathbb{K}u$ est un vecteur directeur de $\mathbb{K}u$, c'est-à-dire que : $v \in \mathbb{K}u \setminus \{0_E\} \iff \mathbb{K}u = \mathbb{K}v$.

∗ Montrons $\Longrightarrow$
Soit $v \in \mathbb{K}u \setminus \{0_E\}$: il existe $\mu \in \mathbb{K}^\star$ tel que $v = \mu \cdot u$. On a alors :

$$\begin{aligned} x \in \mathbb{K}u &\iff \exists \lambda \in \mathbb{K} \ , \ x = \lambda \cdot u \\ &\iff \exists \lambda \in \mathbb{K} \ , \ x = (\lambda \times \mu^{-1}) \cdot v \\ &\iff \exists \lambda' \in \mathbb{K} \ , \ x = \lambda' \cdot v \\ &\iff x \in \mathbb{K}v \end{aligned}$$

d'où $\mathbb{K}u = \mathbb{K}v$.

∗ Montrons $\Longleftarrow$
On suppose que $\mathbb{K}u = \mathbb{K}v$. Alors, d'une part, $v \in \mathbb{K}v = \mathbb{K}u$ et d'autre part, $u \in \mathbb{K}u = \mathbb{K}v$ donc il existe $\lambda \in \mathbb{K}$ tel que $u = \lambda \cdot v$. Par hypothèse, $u \neq 0_E$ donc $\lambda \neq 0_{\mathbb{K}}$ et $v \neq 0_E$. Par suite, $v \in \mathbb{K}u \setminus \{0_E\}$.

⊠

4.2 Opérations sur les espaces vectoriels

4.2.1 Intersection et sous-espace engendré par une partie

Proposition 4.2.1.1 *Soient E un $\mathbb{K}$-espace vectoriel et $(F_i)_{i \in I}$ une famille quelconque de sous-espaces vectoriels de E. Alors $\bigcap_{i \in I} F_i$ est un sous-espace vectoriel de E.*

Preuve :

On applique la définitions.

- Soit $i \in I$. F_i est un sous-espace vectoriel de E donc $0_E \in F_i$. Ceci est vrai pour tout $i \in I$ donc $0_E \in \bigcap_{i\in I} F_i$.
- Soient $\lambda, \mu \in \mathbb{K}$ et $u, v \in \bigcap_{i\in I} F_i$. Soit $i \in I$. Puisque F_i est un sous-espace vectoriel de E, $\lambda \cdot u + \mu \cdot v \in F_i$. Ceci étant vrai pour tout $i \in I$, on en déduit que :

$$\lambda \cdot u + \mu \cdot v \in \bigcap_{i\in I} F_i$$

Ce qui prouve que $\bigcap_{i\in I} F_i$ est bien un sous-espace vectoriel de E.

⊠

Exemple 4.2.1.2 L'ensemble $F = \{f \in \mathcal{C}^0(\mathbb{R}, \mathbb{R}) \ / \ \forall n \in \mathbb{Z}\ ,\ f(n) = 0\}$ est un sous-espace vectoriel de $E = \mathcal{C}^0(\mathbb{R}, \mathbb{R})$. En effet, pour $n \in \mathbb{Z}$, $F_n = \{f \in E \ / \ f(n) = 0\}$ est un sous-espace vectoriel de E donc $F = \bigcap_{n\in\mathbb{Z}} F_n$ est un sous-espace vectoriel de E.

Exemple 4.2.1.3 Dans $\mathbb{R}^3$, les ensembles $\mathcal{P}_1 = \{(x, y, z) \in \mathbb{R}^3 \ / \ x + y + z = 0\}$ et $\mathcal{P}_2 = \{(x, y, z) \in \mathbb{R}^3 \ / \ x - y + z = 0\}$ sont des sous-espaces vectoriels de $\mathbb{R}^3$ (voir l'exemple 4.1.3.7). Par suite,

$$\mathcal{D} = \mathcal{P}_1 \cap \mathcal{P}_2 = \{(x, y, z) \in \mathbb{R}^3 \ / \ x + y + z = x - y + z = 0\}$$

est un sous-espace vectoriel de $\mathbb{R}^3$.

Remarque : *dans l'exemple précédent, on peut aussi prouver directement que $\mathcal{D}$ est une « droite vectorielle ». En effet, soit $(x, y, z) \in \mathbb{R}^3$. On a alors :*

$$\begin{aligned}
(x, y, z) \in \mathcal{D} &\iff \left\{ \begin{array}{rcll} 0 &=& x + y + z & L_1 \\ 0 &=& x - y + z & L_2 \end{array} \right. \\
&\iff \left\{ \begin{array}{rcll} y &=& 0 & L_1 \longleftarrow L_1 - L_2 \\ z &=& -x & L_2 \end{array} \right. \\
&\iff (x, y, z) = x(1, 0, -1) \\
&\iff (x, y, z) \in \mathbb{R}(1, 0, -1)
\end{aligned}$$

Ce qui montre que $\mathcal{D} = \mathbb{R}u$ avec $u = (1, 0, -1)$ et donc $\mathcal{D}$ est une bien un sous-espace vectoriel de $\mathbb{R}^3$. Dans l'exemple, on a utilisé un système d'équations cartésiennes de $\mathcal{D}$

alors que dans la remarque, on a donné une représentation paramétrique de $\mathcal{D}$ (vous devez impérativement savoir donner les deux formes).

⚠ **Attention :** en revanche, une erreur très grave et très classique est de dire que la réunion de deux sous-espaces vectoriels est un sous-espace vectoriel.
En général, la réunion de deux sous-espaces vectoriels n'est pas un sous-espace vectoriel.

Exemple 4.2.1.4 Dans le plan usuel par exemple, $F = \mathbb{R}\vec{i}$ et $G = \mathbb{R}\vec{j}$ sont des sous-espaces vectoriels de $\overrightarrow{\mathcal{P}}$. Pourtant, $F \cup G$ n'est pas un espace vectoriel puisque par exemple, $\vec{i} \in F \cup G$, $\vec{j} \in F \cup G$ mais $\vec{i} + \vec{j} \notin F \cup G$ (puisque $\vec{i}$ et $\vec{j}$ ne sont pas colinéaires).

Définition 4.2.1.5 Soient E un $\mathbb{K}$-ev et $X \subset E$ une partie quelconque de E. On appelle espace vectoriel engendré par X, et on note $Vect(X)$ ou $< X >$, l'ensemble défini par :

$$< X > \; = \bigcap_{\substack{X \subset F \\ F \text{ sev } E}} F$$

Proposition 4.2.1.6 *Pour toute partie $X \subset E$, $< X >$ est un sous-espace vectoriel de E et c'est le plus petit sous-espace vectoriel de E (pour l'inclusion) qui contient X.*

Preuve :

D'après la proposition précédente, $< X >$ est bien un sous-espace vectoriel puisque c'est une intersection de sous-espaces vectoriels de E.
Par ailleurs, si G est un sous-espace vectoriel de E qui contient X, alors $G \in \{F \text{ sev de } E \ / \ X \subset F\}$. Par conséquent, $\bigcap_{\substack{X \subset F \\ F \text{ sev } E}} F \subset G$, c'est-à-dire $< X > \subset G$.

⊠

Exemple 4.2.1.7 Soient E un $\mathbb{K}$-espace vectoriel et $X = \emptyset$: déterminons $< X >$.

- D'une part, $\{0_E\}$ est bien un sous-espace vectoriel de E qui contient X donc $< X > \subset \{0_E\}$.
- D'autre part, comme $< X >$ est un sous-espace vectoriel de E, il contient 0_E donc $\{0_E\} \subset < X >$.

Ainsi, par double inclusion, $< \emptyset >= \{0_E\}$.

Exemple 4.2.1.8 Soient E un $\mathbb{K}$-espace vectoriel et $u \in E \setminus \{0_E\}$. Alors $< \{u\} >= \mathbb{K}u$.

- On a déjà prouvé que $\mathbb{K}u$ est un sous-espace vectoriel de E et par définition, $u \in \mathbb{K}u$. Par conséquent, $< \{u\} > \subset \mathbb{K}u$.
- Réciproquement, si F est un sous-espace vectoriel de E qui contient $\{u\}$, c'est-à-dire $u \in F$, alors pour tout $\lambda \in \mathbb{K}$, $\lambda \cdot u \in F$ (car F est un sous-espace vectoriel). Par suite $\mathbb{K}u \subset F$. Par conséquent, $\mathbb{K}u \subset < \{u\} >$.

Proposition 4.2.1.9 *Soit E un $\mathbb{K}$-espace vectoriel et soit X une partie quelconque de E. Alors X est un sous-espace vectoriel de E si et seulement si $< X >= X$.*

Preuve :

• Montrons l'implication directe.
Si X est un sous-espace vectoriel de E, alors d'une part $X \subset < X >$ (par définition de l'espace vectoriel engendré par une partie) et d'autre part, X est alors un sous-espace vectoriel de E qui contient X, par suite $< X > \subset X$. Finalement, $X =< X >$.

• Réciproquement, si $X =< X >$, alors X est un sous-espace vectoriel de E car $< X >$ l'est.

⊠

Remarques et notations :

- *à partir de la définition, ce qu'on utilise dans la pratique, c'est la propriété suivante : « si F est un sous-espace vectoriel de E contenant X, alors $< X > \subset F$ » ;*
- *par abus, on notera $< \{u\} >=< u >$. Plus généralement, par abus toujours, si X est une partie finie non vide, $X = \{x_1, \cdots, x_n\}$, on notera :*

$$Vect(X) =< X >=< x_1, \cdots, x_n >= Vect(x_1, \cdots, x_n)$$

Le seul « problème » avec la définition est qu'elle ne permet pas en général de déterminer explicitement $< X >$. Pour cela, on dispose du théorème fondamental suivant.

Théorème 4.2.1.10 *Soient E un $\mathbb{K}$-espace vectoriel et $X \subset E$, avec $X \neq \emptyset$. Alors l'espace vectoriel engendré par X est l'ensemble des combinaisons linéaires d'éléments de X. Autrement dit, $u \in Vect(X)$ si et seulement si*

$$\exists n \in \mathbb{N} \ , \ \exists (x_0, \cdots, x_n) \in X^{n+1} \ , \ \exists (\lambda_0, \cdots, \lambda_n) \in \mathbb{K}^{n+1} \ , \ u = \sum_{k=0}^{n} \lambda_k \cdot x_k$$

► À retenir :

En clair, il faut retenir que :

$$< X >= \left\{ \sum_{k=0}^{n} \lambda_k x_k \ , \ n \in \mathbb{N} \text{ et } \forall k \in [\![0, n]\!] \ , \ \lambda_k \in \mathbb{K} \text{ et } x_k \in X \right\}$$

Preuve :

Pour simplifier les notations, on donne ci-dessous la preuve dans le cas où X est une partie **finie** non vide de E. La preuve repose sur le même principe dans le cas où X est éventuellement une partie infinie.
Ainsi, on note $X = \{x_k \ , \ 0 \leqslant k \leqslant n\}$, où n est un entier naturel fixé.
Notons G l'ensemble des combinaisons linéaires des éléments de X, c'est-à-dire :

$$G = \left\{ \sum_{k=0}^{n} \lambda_k x_k \ / \ \forall k \in [\![0, n]\!] \ , \ \lambda_k \in \mathbb{K} \right\}$$

• Montrons que $G \subset < X >$.
D'après la proposition précédente, $< X >$ est un sous-espace vectoriel de E qui contient les éléments de X. Par conséquent, il contient toute combinaison linéaire d'éléments de X, c'est-à-dire $G \subset < X >$.

• Montrons à présent que $< X > \subset G$.
Pour cela, on montre que G est un sous-espace vectoriel de E. Comme $X \subset G$ on aura alors $< X > \subset G$ (puisque $< X >$ est le plus petit sous-espace vectoriel de E qui contient X).

- ∗ Par hypothèse, $X \neq \emptyset$: soit $x \in X$. Alors $0_{\mathbb{K}} \cdot x \in G$, c'est-à-dire $0_E \in G$.
- ∗ Soient $u, v \in G$ et $\lambda, \mu \in \mathbb{K}$. Par définition de l'ensemble G, il existe $(\lambda'_k)_{0 \leqslant k \leqslant n} \in \mathbb{K}^{n+1}$ et $(\lambda''_k)_{0 \leqslant k \leqslant n} \in \mathbb{K}^{n+1}$ tels que :

$$u = \sum_{k=0}^{n} \lambda'_k \cdot x_k \quad \text{et} \quad v = \sum_{k=0}^{n} \lambda''_k \cdot x_k$$

Posons pour tout $k \in [\![0, n]\!]$, $\lambda_k = \lambda\lambda'_k + \mu\lambda''_k \in \mathbb{K}$. On a alors :

$$\lambda \cdot u + \mu \cdot v = \sum_{k=0}^{n} \lambda_k \cdot x_k \in G$$

Ce qui prouve que G est un sous-espace vectoriel de E, terminant ainsi la démonstration.

⊠

Remarque : *lorsque X est une partie infinie, la seule différence dans la démonstration est la preuve que G est stable par combinaisons linéaires. En effet, si l'on se donne deux éléments $u \in G$ et $v \in G$, alors u et v s'écrivent sous la forme :*

$$u = \sum_{k=0}^{n} \lambda'_k x'_k \quad et \quad v = \sum_{k=0}^{p} \lambda''_k x''_k$$

avec $n \in \mathbb{N}$ et $p \in \mathbb{N}$ (mais n et p ne sont dans ce cas pas nécessairement égaux), $(x'_0, \cdots, x'_n) \in X^{n+1}$, $(x''_0, \cdots, x''_p) \in X^{p+1}$, $(\lambda'_0, \cdots, \lambda'_n) \in \mathbb{K}^{n+1}$ et $(\lambda''_0, \cdots, \lambda''_p) \in \mathbb{K}^{p+1}$. Autrement dit, les combinaisons linéaires ne contiennent pas forcément le même nombre de vecteurs, ni même les mêmes vecteurs. L'écriture est donc un peu plus délicate mais l'idée est la même. Pour $(\lambda, \mu) \in \mathbb{K}^2$, on pose :

$$\forall k \in [\![0, n+p+1]\!] \ , \ x_k = \begin{cases} x'_k & si\ 0 \leqslant k \leqslant n \\ x''_{k-(n+1)} & si\ n+1 \leqslant k \leqslant n+p+1 \end{cases}$$

et

$$\forall k \in [\![0, n+p+1]\!] \ , \ \lambda_k = \begin{cases} \lambda\lambda'_k & si\ 0 \leqslant k \leqslant n \\ \mu\lambda''_{k-(n+1)} & si\ n+1 \leqslant k \leqslant n+p+1 \end{cases}$$

De cette façon, on a :

$$\lambda \cdot u + \mu \cdot v = \sum_{k=0}^{n+p+1} \lambda_k x_k$$

Vous verrez plus tard (dans le cours de mathématiques spéciales 1) une méthode de notation qui permet de simplifier cette écriture technique. Mais pour ce chapitre, vous devez simplement maîtriser les écritures (et les preuves) lorsque X est une partie finie non vide de E.

Exemple 4.2.1.11 Si u est un vecteur de E, on retrouve que $\text{Vect}(u) = \mathbb{K} \cdot u$. Notez bien que si $u = 0_E$, alors $\mathbb{K}u = \{0_E\}$, ce qui est logique puisque le plus petit sous-espace vectoriel de E qui contient 0_E est $\{0_E\}$.

Exemple 4.2.1.12 Si u et v sont deux vecteurs non colinéaires, alors $< u, v >$ est le plan vectoriel engendré par u et v, c'est-à-dire l'ensemble des combinaisons linéaires de u et v. On écrira aussi $< u, v >= \mathbb{K}u + \mathbb{K}v$ ou plus exactement, $< u, v >= \mathbb{K}u \oplus \mathbb{K}v$ lorsque u et v sont non colinéaires (voir paragraphes suivants).

Exemple 4.2.1.13 L'ensemble $\mathcal{S}$ des suites réelles $(u_n)_{n\in\mathbb{N}}$ vérifiant la relation de récurrence :

$$\forall n \in \mathbb{N} \ , \ u_{n+2} - 5u_{n+1} + 6u_n = 0$$

est $\mathcal{S} = \text{Vect}((2^n)_{n\in\mathbb{N}}, (3^n)_{n\in\mathbb{N}})$. En effet, les racines du polynôme caractéristique associé étant 2 et 3, on a démontré que si $(u_n)_{n\in\mathbb{N}} \in \mathbb{R}^{\mathbb{N}}$, alors :

$$(u_n)_{n\in\mathbb{N}} \in \mathcal{S} \iff \exists (\lambda, \mu) \in \mathbb{R}^2 \ , \ (u_n)_{n\in\mathbb{N}} = \lambda(2^n)_{n\in\mathbb{N}} + \mu(3^n)_{n\in\mathbb{N}}$$

Exemple 4.2.1.14 De même, l'ensemble des solutions de l'équation $y'' + y = 0$ est $< \sin, \cos >$. Ceci permet d'ailleurs de justifier que cet ensemble est un espace vectoriel car c'est l'espace vectoriel engendré par $\{\cos, \sin\} \subset \mathcal{F}(\mathbb{R}, \mathbb{R})$.

Exemple 4.2.1.15 L'ensemble $\mathcal{P}$ des fonctions polynomiales sur $\mathbb{R}$ est par définition $\mathcal{P} = \text{Vect}(\{x \mapsto x^n \ , \ n \in \mathbb{N}\})$. En effet, par définition, f est une fonction polynomiale (sur $\mathbb{R}$) si et seulement si il existe $n \in \mathbb{N}$, $(a_0, \cdots, a_n) \in \mathbb{R}^{n+1}$ tels que :

$$\forall x \in \mathbb{R} \ , \ f(x) = \sum_{k=0}^{n} a_k x^k$$

c'est-à-dire si et seulement si il existe $n \in \mathbb{N}$, $(a_0, \cdots, a_n) \in \mathbb{R}^{n+1}$ tels que :

$$f = \sum_{k=0}^{n} a_k (x \longmapsto x^k)$$

soit encore si et seulement si f est une combinaison linéaire d'éléments de l'ensemble $\{x \mapsto x^n \ , \ n \in \mathbb{N}\}$.

Exemple 4.2.1.16 L'ensemble des polynômes trigonométriques (2π-périodiques) est par définition :

$$\text{Vect}(\{x \mapsto \cos(nx) \ , \ n \in \mathbb{N}\} \cup \{x \mapsto \sin(nx) \ , \ n \in \mathbb{N}^\star\})$$

C'est un sous-espace vectoriel de l'ensemble des fonctions de $\mathbb{R}$ dans $\mathbb{R}$, 2π-périodiques.

⚠ **Attention :** par définition, une combinaison linéaire est toujours une somme **finie** ! Le nombre de termes dans cette somme peut être arbitrairement grand mais il reste fini ! Essentiellement, il y a deux raisons :

- tout d'abord, si l'on écrit $\sum_{n=0}^{+\infty} \lambda_n \cdot x_n$, ce n'est qu'une notation ! Cela désigne la limite de la suite $(S_n) = \left(\sum_{k=0}^{n} \lambda_k \cdot x_k \right)$. Or, vous n'avez pas encore étudié la notion de limite pour une suite d'éléments de E lorsque E est un espace vectoriel quelconque. En fait, vous verrez (comme dans le paragraphe d'applications aux séries à termes positifs de ce livre) que cette notation suppose la convergence, ce qui n'a aucune raison d'être le cas quand on fait une combinaison linéaire quelconque ;
- ensuite, un espace vectoriel est stable par addition de deux termes. On a ensuite montré que ceci entraîne qu'il est stable par addition d'un nombre fini de termes. Mais il n'y a aucune raison pour que la limite (c'est-à-dire une somme infinie de

termes) appartienne encore à l'espace. Par exemple, on montrera dans le cours d'intégration (cours de mathématiques supérieures 2) que :

$$\forall x \in \mathbb{R}\ ,\ \exp(x) = \sum_{n=0}^{+\infty} \frac{1}{n!} x^n$$

Autrement écrit, $\exp = \sum_{n=0}^{+\infty} \frac{1}{n!}(x \longmapsto x^n)$ mais portant la fonction exponentielle n'est pas une fonction polynomiale (car ses dérivées successives ne sont jamais identiquement nulles), c'est-à-dire

$$\sum_{n=0}^{+\infty} \frac{1}{n!}(x \longmapsto x^n) \notin \text{Vect}\left(\{x \longmapsto x^n\ ,\ n \in \mathbb{N}\}\right)$$

Remarque : *à nouveau, dans ce livre, ce ne sera pas gênant car on travaillera toujours (ou presque) avec X une partie finie non vide et de plus, n'ayant pas encore étudié les séries en général, vous ne devez pas être tentés d'écrire des sommes infinies pour le moment. La mise en garde précédente est essentielle pour les cours ultérieurs (en particulier pour les cours de mathématiques spéciales 1 et 2).*

4.2.2 Somme de sous-espaces vectoriels

Définition 4.2.2.1 Soit E un $\mathbb{K}$-espace vectoriel et soient F et G deux sous-espaces vectoriels de E. On définit la somme de F et G, notée $F+G$, par :

$$F + G = \{u \in E\ /\ \exists (x, y) \in F \times G\ ,\ u = x + y\}$$

⚠ **Attention :** $u \in F+G \iff \exists (x,y) \in F \times G\ ,\ u = x+y$ mais x et y ne sont pas nécessairement uniques ! Par exemple, dans l'espace, si $F =< \vec{i}, \vec{j} >$ et $G =< \vec{i}+\vec{j}, \vec{k} >$ on a :

$$\vec{u} = \underbrace{\vec{0}}_{\text{dans } F} + \underbrace{\vec{i}+\vec{j}}_{\text{dans } G} = \underbrace{\vec{i}+\vec{j}}_{\text{dans } F} + \underbrace{\vec{0}}_{\text{dans } G}$$

Proposition 4.2.2.2 *Avec les hypothèses de la définition, $F+G$ est un sous-espace vectoriel de E. De plus, c'est le plus petit sous-espace vectoriel de E contenant F et G, c'est-à-dire que $F+G = Vect(F \cup G)$.*

Preuve :

Montrons directement que $F+G = \text{Vect}(F \cup G)$, ce qui prouvera également que $F+G$ est un sous-espace vectoriel de E.

• Montrons que $F+G \subset \text{Vect}(F \cup G)$.
Soit $u \in F+G$. Par définition, il existe $x \in F$ et $y \in G$ tels que $u = x+y$. On a alors $u = 1_{\mathbb{K}} \cdot x + 1_{\mathbb{K}} \cdot y$ avec $(x,y) \in (F \cup G)^2$ et $(1_{\mathbb{K}}, 1_{\mathbb{K}}) \in \mathbb{K}^2$ donc $u \in < F \cup G >$, ce qui prouve la première inclusion.

• Montrons à présent que $< F \cup G > \subset F+G$.
Soit $u \in < F \cup G >$. Par définition de l'espace vectoriel engendré par une partie, il existe $n \in \mathbb{N}$, $(x_i)_{0 \leqslant i \leqslant n} \in (F \cup G)^{n+1}$ et $(\lambda_i)_{0 \leqslant i \leqslant n} \in \mathbb{K}^{n+1}$ tels que :

$$u = \sum_{i=0}^{n} \lambda_i x_i$$

On pose $I = \{i \in [\![0,n]\!] \ / \ x_i \in F\}$ et $J = [\![0,n]\!] \setminus I$. On a alors :

$$u = \sum_{i \in I} \lambda_i x_i \ + \ \sum_{j \in J} \lambda_j x_j$$

Or, pour tout $i \in I$, $x_i \in F$, I est un ensemble fini et F est un sous-espace vectoriel de E. Par suite,

$$x = \sum_{i \in I} \lambda_i x_i \in F$$

De même, pour tout $j \in J$, $x_j \in G \setminus F \subset G$ et G est un sous-espace vectoriel de E donc :

$$y = \sum_{j \in J} \lambda_j x_j \in G$$

Notez bien que si $I = \emptyset$ ou $J = \emptyset$, le résultat est encore valable puisque $\sum_{i \in \emptyset} \lambda_i x_i = 0_E$ qui appartient bien à F (et à G).
Ainsi, $u = x+y$ avec $x \in F$ et $y \in G$, c'est-à-dire $u \in F+G$. D'où la seconde inclusion.

⊠

Exemple 4.2.2.3 Si u et v sont deux vecteurs non colinéaires, $\mathbb{K}u + \mathbb{K}v$ est le plan vectoriel engendré par u et v.

⚠ **Attention :** ne pas se laisser abuser par les notations !! $F+F = F$ et $F-F = F$!!

⚠ **Attention :** on rappelle une fois de plus que $F \cup G$ n'est pas un espace vectoriel en général.

On peut généraliser la définition à une somme finie de sous-espaces vectoriels de E.

Définition 4.2.2.4 Soient E un $\mathbb{K}$-espace vectoriel, $n \in \mathbb{N}^\star$ et pour tout $i \in [\![1, n]\!]$, F_i un sous-espace vectoriel de E. On appelle somme des F_i pour $1 \leqslant i \leqslant n$, et on note $\sum_{i=1}^{n} F_i$, l'ensemble défini par :

$$\begin{aligned}\sum_{i=1}^{n} F_i &= F_1 + F_2 + \cdots + F_n \\ &= \left\{ \sum_{i=1}^{n} u_i \ / \ \forall i \in [\![1, n]\!] \ , \ u_i \in F_i \right\} \\ &= \{u_1 + u_2 + \cdots + u_n \ / \ \forall i \in [\![1, n]\!] \ , \ u_i \in F_i\}\end{aligned}$$

Autrement dit, pour $x \in E$ quelconque,

$$x \in \sum_{i=1}^{n} F_i \iff \exists (u_i)_{1 \leqslant i \leqslant n} \in \prod_{i=1}^{n} F_i \ , \ x = \sum_{i=1}^{n} u_i$$

Remarque : *cette définition a un sens et il n'y a pas d'ambiguïté dans la définition puisque l'addition dans E est commutative et associative. Autrement dit, pour toute permutation de $[\![1, n]\!]$, $\sum_{i=1}^{n} F_i = \sum_{i=1}^{n} F_{\sigma(i)}$ et il n'est pas nécessaire de préciser dans quel ordre on fait les additions et de plus, si $I \sqcup J = [\![1, n]\!]$, alors :*

$$\left(\sum_{i \in I} F_i \right) + \left(\sum_{i \in J} F_i \right) = \sum_{i=1}^{n} F_i$$

Exemple 4.2.2.5 Si on note $\overrightarrow{\mathcal{E}}$ l'espace habituel, on a : $\mathbb{R}\vec{i} + \mathbb{R}\vec{j} + \mathbb{R}\vec{k} = \overrightarrow{\mathcal{E}}$.

Exemple 4.2.2.6 Si on note pour $n \in \mathbb{N}$, $F_n = < x \longmapsto x^n >$, alors $\sum_{i=0}^{n} F_i$ est l'ensemble des fonctions polynomiales de degré inférieur ou égal à n.

Exercice 4.2.2.7 On note $u = (1, 0, 0)$, $v = (1, 1, 0)$ et $w = (1, 1, 1)$. Montrer de deux façons différentes que $\mathbb{R}u + \mathbb{R}v + \mathbb{R}w = \mathbb{R}^3$. *On pourra pour l'une des méthodes utiliser le déterminant de trois vecteurs de l'espace « usuel ».*

Proposition 4.2.2.8 *Soient E un $\mathbb{K}$-espace vectoriel, $n \in \mathbb{N}^\star$ et pour tout $i \in [\![1, n]\!]$, F_i un sous-espace vectoriel de E. Alors, $\sum_{i=1}^{n} F_i$ est un sous-espace vectoriel de E et de plus, $\sum_{i=1}^{n} F_i = Vect\left(\bigcup_{i=1}^{n} F_i\right)$, c'est-à-dire que $\sum_{i=1}^{n} F_i$ est le plus petit sous-espace vectoriel de E qui contient tous les F_i pour $1 \leqslant i \leqslant n$.*

Preuve :

• Montrons que $F = \sum_{i=1}^{n} F_i$ est bien un sous-espace vectoriel de E et qu'il contient chacun des F_i (pour $1 \leqslant i \leqslant n$).

∗ Pour tout $i \in [\![1, n]\!]$, $0_E \in F_i$ (car F_i est un sous-espace vectoriel de E. Par suite, en posant $u_i = 0_E$, on a $u_i \in F_i$ et donc :

$$\sum_{i=1}^{n} u_i \in \sum_{i=1}^{n} F_i \quad \text{c'est-à-dire} \quad 0_E \in \sum_{i=1}^{n} F_i$$

∗ Soient $(x, y) \in F^2$ et $(\lambda, \mu) \in \mathbb{K}^2$. Puisque $x \in F$ et $y \in F$, il existe $(u_i)_{1\leqslant i\leqslant n} \in \prod_{i=1}^{n} F_i$ et $(v_i)_{1\leqslant i\leqslant n} \in \prod_{i=1}^{n} F_i$ tels que :

$$x = \sum_{i=1}^{n} u_i \quad \text{et} \quad y = \sum_{i=1}^{n} v_i$$

On a alors :

$$\begin{aligned} \lambda \cdot x + \mu \cdot y &= \lambda \cdot \left(\sum_{i=1}^{n} u_i\right) + \mu \cdot \left(\sum_{i=1}^{n} v_i\right) \\ &= \sum_{i=1}^{n} \lambda \cdot u_i + \sum_{i=1}^{n} \mu \cdot v_i \\ &= \sum_{i=1}^{n} (\lambda \cdot u_i + \mu \cdot v_i) \end{aligned}$$

Or, pour tout $i \in [\![1, n]\!]$, $\lambda \cdot u_i + \mu \cdot v_i \in F_i$ (car F_i est un sous-espace vectoriel de E). Par conséquent, $\lambda \cdot x + \mu \cdot y \in F$.

Ce qui prouve que $F = \sum_{i=1}^{n} F_i$ est un sous-espace vectoriel de E.

De plus, soient $i \in [\![1,n]\!]$ et $x \in F_i$, alors en posant $u_j = 0_E$ si $j \neq i$ et $u_i = x$, on a :

$$x = \sum_{j=1}^{n} u_j \quad \text{et} \quad \forall j \in [\![1,n]\!] \ , \ u_j \in F_j$$

Ce qui montre que $x \in F$ et donc finalement $F_i \subset F$.

• Ensuite, puisque $F = \sum_{i=1}^{n} F_i$ est un sous-espace vectoriel de E qui contient F_i pour tout $1 \leqslant i \leqslant n$, il contient aussi $\bigcup_{i=1}^{n} F_i$. Par suite, l'inclusion $\text{Vect}(\bigcup_{i=1}^{n} F_i) \subset \sum_{i=1}^{n} F_i$ est claire.
Réciproquement, soit $x \in F$. Il existe $(u_1, \cdots, u_n) \in \prod_{i=1}^{n} F_i$ tel que : $x = \sum_{i=1}^{n} u_i$. Pour tout $i \in [\![1,n]\!]$, $x_i \in F_i \subset \text{Vect}(\bigcup_{i=1}^{n} F_i)$. Par suite, $\sum_{i=1}^{n} x_i \in \text{Vect}(\bigcup_{i=1}^{n} F_i)$ (puisque ce dernier est un sous-espace vectoriel de E et est donc stable par combinaisons linéaires). Par conséquent, $x \in \text{Vect}(\bigcup_{i=1}^{n} F_i)$, c'est-à-dire $\sum_{i=1}^{n} F_i \subset \text{Vect}(\bigcup_{i=1}^{n} F_i)$.

⊠

4.2.3 Sommes directes et sous-espaces vectoriels supplémentaires

Définition 4.2.3.1 Soient E un $\mathbb{K}$-espace vectoriel et F, G deux sous-espaces vectoriels de E. On dit que F et G sont en somme directe si $F \cap G = \{0_E\}$. Dans ce cas, la somme de F et G est notée $F \oplus G$.

⚠ **Attention :** vous ne devez jamais écrire $F \oplus G$ sans avoir d'abord démontré que F et G sont en somme directe, c'est-à-dire sans avoir prouvé que $F \cap G = \{0_E\}$! ! !

Proposition 4.2.3.2 *Soient E un $\mathbb{K}$-espace vectoriel et F, G deux sous-espaces vectoriels de E. Alors les propriétés suivantes sont équivalentes :*

(i) F et G sont en somme directe ;

(ii) tout élément u de $F+G$ se décompose de façon unique sous la forme $u = x+y$ avec $x \in F$ et $y \in G$, c'est-à-dire $\forall u \in F+G$, $\exists!(x,y) \in F \times G$, $u = x+y$.

Preuve :

• Montrons $(i) \Longrightarrow (ii)$.

On suppose que F et G sont en somme directe : $F \cap G = \{0_E\}$.

∗ Tout d'abord, il est clair, par définition de l'ensemble $F+G$, que :

$$\forall u \in F+G \ , \ \exists (x,y) \in F \times G \ , \ u = x+y$$

∗ On doit donc prouver l'unicité. Supposons que $x+y = x'+y'$ avec $(x,y),(x',y') \in F \times G$. Alors, $x-x' = y'-y$. Or, $x, x' \in F$ et F est un sous-espace vectoriel de E donc $x-x' \in F$. De la même façon, $y'-y \in G$. Par conséquent, $(x-x') \in F \cap G = \{0_E\}$. Il s'ensuit que $x = x'$ et donc $y = y'$, prouvant ainsi l'unicité de la décomposition.

• Montrons $(ii) \Longrightarrow (i)$.

On suppose (ii). Soit $x \in F \cap G$. Alors, par exemple, $(-x) \in G$. Il s'ensuit que $0_E = x + (-x)$ avec $x \in F$ et $(-x) \in G$. Or, on a également $0_E \in F \cap G$: on peut donc aussi écrire $0_E = 0_E + 0_E$ avec $(0_E, 0_E) \in F \times G$. D'après (ii), la décomposition est unique : ceci implique que $x = 0_E$, prouvant ainsi que $F \cap G = \{0_E\}$.

⊠

Définition 4.2.3.3 Soient E un $\mathbb{K}$-espace vectoriel et F, G deux sous-espaces vectoriels de E. On dit que F et G sont supplémentaires (ou supplémentaires dans E) si tout vecteur de E peut se décomposer de façon unique en la somme d'un vecteur de F et d'un vecteur de G. Autrement dit F et G sont supplémentaires si :

$$\forall u \in E \ , \ \exists ! (x,y) \in F \times G \ , \ u = x+y$$

Exemple 4.2.3.4 Dans le plan vectoriel, $\mathbb{K}\vec{i}$ et $\mathbb{K}\vec{j}$ sont supplémentaires, tout comme $\mathbb{K}\vec{i}$ et $\mathbb{K}(\vec{i}+\vec{j})$.

Théorème 4.2.3.5 *Deux sous-espaces vectoriels F et G sont supplémentaires (dans E) si et seulement si*

$$F+G = E \qquad et \qquad F \cap G = \{0\}$$

c'est-à-dire si et seulement si $F \oplus G = E$.

Preuve :

• Montrons $\Longrightarrow$.
On suppose que F et G supplémentaires. Alors, pour $u \in E$, il existe $x \in F$ et $y \in G$ tels que $u = x + y$ donc $F + G = E$. Par ailleurs, cette décomposition étant unique par définition de deux sous-espaces vectoriels supplémentaires, la proposition précédente montre que F et G sont en somme directe, c'est-à-dire $F \cap G = \{0_E\}$.

• Montrons $\Longleftarrow$.
On suppose que $F \oplus G = E$. Alors d'une part, $F + G = E$: ce qui prouve que tout élément de E s'écrit comme la somme d'un élément de F et d'un élément de G. Et d'autre part, $F \oplus G$: donc d'après la proposition précédente, cette écriture est unique.

⊠

Exemple 4.2.3.6 On se place dans $E = \mathbb{R}^3$ et on considère les vecteurs $u = (1, 0, 1)$, $v = (1, 1, -1)$ et $w = (1, -1, 0)$. On pose $F =< u, v >$ et $G =< v >$. Montrons que F et G sont supplémentaires dans $\mathbb{R}^3$.

• Première méthode
On veut montrer que tout élément de $\mathbb{R}^3$ s'écrit de façon unique comme la somme d'un élément de F et d'un élément de G. Soit $(x, y, z) \in \mathbb{R}^3$.

$$\begin{aligned}
(x,y,z) \in F+G &\iff \exists (a,b) \in F \times G \ , \ (x,y,z) = a+b \\
&\iff \exists (\lambda,\mu,\gamma) \in \mathbb{R}^3 \ , \ (x,y,z) = \lambda u + \mu v + \gamma v \\
&\iff \exists (\lambda,\mu,\gamma) \in \mathbb{R}^3 \ , \ \left\{ \begin{array}{rcl} x & = & \lambda + \mu + \gamma \\ y & = & \mu - \gamma \\ z & = & \lambda - \mu \end{array} \right. \\
&\iff \exists (\lambda,\mu,\gamma) \in \mathbb{R}^3 \ , \ \left\{ \begin{array}{rcl} x & = & \lambda + \mu + \gamma \\ \gamma & = & \mu - y \\ \lambda & = & \mu + z \end{array} \right. \\
&\iff \exists (\lambda,\mu,\gamma) \in \mathbb{R}^3 \ , \ \left\{ \begin{array}{rcl} 3\mu & = & x + y - z \\ \gamma & = & \mu - y \\ \lambda & = & \mu + z \end{array} \right. \\
&\iff \exists (\lambda,\mu,\gamma) \in \mathbb{R}^3 \ , \ \left\{ \begin{array}{rcl} \mu & = & \frac{1}{3}x + \frac{1}{3}y - \frac{1}{3}z \\ \gamma & = & \frac{1}{3}x - \frac{2}{3}y - \frac{1}{3}z \\ \lambda & = & \frac{1}{3}x + \frac{1}{3}y + \frac{2}{3}z \end{array} \right.
\end{aligned}$$

Ceci montre que tout élément $(x, y, z) \in \mathbb{R}^3$ s'écrit de façon unique :

$$(x,y,z) = \left(\left(\frac{1}{3}x + \frac{1}{3}y + \frac{2}{3}z\right)u + \left(\frac{1}{3}x + \frac{1}{3}y - \frac{1}{3}z\right)v\right) + \left(\frac{1}{3}x - \frac{2}{3}y - \frac{1}{3}z\right)w$$

Par conséquent, $F \oplus G = \mathbb{R}^3$.

- Seconde méthode

  Il est parfois un peu délicat de conserver des équivalences tout au long du raisonnement (ou difficile à rédiger). Dans ce cas, une méthode générale est de procéder par analyse-synthèse. L'analyse montrera que sous réserve d'existence, on a unicité de la décomposition et la synthèse prouvera l'existence.

  Analyse

  Soit $(x, y, z) \in \mathbb{R}^3$. On suppose qu'il existe $(a, b) \in F \times G$ tel que $(x, y, z) = a + b$. Puisque $a \in F$ (respectivement $b \in G$), il existe $(\lambda, \mu) \in \mathbb{R}^2$ (respectivement $\gamma \in \mathbb{R}$) tel que $a = \lambda u + \mu v$ (respectivement $b = \gamma w$). On a alors :

  $$\left\{ \begin{array}{rcl} x & = & \lambda + \mu + \gamma \\ y & = & \mu - \gamma \\ z & = & \lambda - \mu \end{array} \right.$$

  D'où l'on déduit que (normalement, on doit faire les calculs mais comme on les a déjà faits dans la méthode 1, ils ne sont pas recopiés ici) :

  $$a = \left(\frac{1}{3}x + \frac{1}{3}y + \frac{2}{3}z\right) u + \left(\frac{1}{3}x + \frac{1}{3}y - \frac{1}{3}z\right) v \quad \text{et} \quad b = \left(\frac{1}{3}x - \frac{2}{3}y - \frac{1}{3}z\right) w$$

  Synthèse

  On pose $a = \left(\frac{1}{3}x + \frac{1}{3}y + \frac{2}{3}z\right) u + \left(\frac{1}{3}x + \frac{1}{3}y - \frac{1}{3}z\right) v$ et $b = \left(\frac{1}{3}x - \frac{2}{3}y - \frac{1}{3}z\right) w$. Alors, $a \in < u, v >= F$, $b \in < w >= G$ et le calcul direct montre que $(x, y, z) = a + b$.

- Troisième méthode

  D'après les propriétés des vecteurs de $\mathbb{R}^3$ (on utilise ici les outils vectoriels dans $\mathbb{R}^2$ et $\mathbb{R}^3$, plus exactement le déterminant),

  $$\det(u, v, w) = \begin{vmatrix} 1 & 1 & 1 \\ 0 & 1 & -1 \\ 1 & -1 & 0 \end{vmatrix} = -3 \neq 0$$

  On en déduit que (u, v, w) est une base de $\mathbb{R}^3$ et donc tout vecteur de l'espace $\mathbb{R}^3$ s'écrit de façon unique comme combinaison linéaire de u, v et w.

  Cette méthode est bien plus rapide mais ne peut pas se généraliser pour le moment (la notion de base d'un espace vectoriel sera étudiée dans le cours de mathématiques supérieures 2) et de toute façon ne s'applique pas dans toutes les situations (lorsque E n'est pas de « dimension finie »).

Exercice 4.2.3.7 On considère $E = \mathcal{F}(\mathbb{R}, \mathbb{R})$, $\mathcal{P} = \{f \in \mathcal{F}(\mathbb{R}, \mathbb{R}) \ / \ f \text{ est paire } \}$ et enfin $\mathcal{I} = \{f \in \mathcal{F}(\mathbb{R}, \mathbb{R}) \ / \ f \text{ est impaire } \}$. On a déjà vu que $P \oplus I = \mathcal{F}(\mathbb{R}, \mathbb{R})$: le reprouver.

Exercice 4.2.3.8 On considère E l'ensemble des applications de $\mathbb{R}$ dans $\mathbb{R}$ qui sont $2T$-périodiques (avec $T > 0$).

1. Montrer que E est un sous-espace vectoriel de $\mathcal{F}(\mathbb{R}, \mathbb{R})$.
2. On note F (respectivement G) l'ensemble des fonctions T-périodiques (respectivement anti-T-périodiques), c'est-à-dire :

$$\begin{aligned} F &= \{f \in \mathcal{F}(\mathbb{R}, \mathbb{R}) \ / \ \forall x \in \mathbb{R} \ , \ f(x+T) = f(x)\} \\ G &= \{f \in \mathcal{F}(\mathbb{R}, \mathbb{R}) \ / \ \forall x \in \mathbb{R} \ , \ f(x+T) = -f(x)\} \end{aligned}$$

   Montrer que F et G sont deux sous-espaces vectoriels supplémentaires dans E.

Remarques :

- *il ne faut pas confondre la notion de supplémentaire et la notion de complémentaire ! F et G sont supplémentaires dans E ne veut pas du tout dire qu'un vecteur de E appartient à F ou à G !*
- *F et G sont en somme directe ne signifie pas que F et G sont supplémentaires ! Autrement dit :*

$$F \oplus G = E \Longrightarrow F \oplus G \quad \textit{mais} \quad F \oplus G \not\Longrightarrow F \oplus G = E$$

- *ne jamais oublier de montrer avant tout que F et G sont des sous-espaces vectoriels de E avant d'essayer de prouver qu'ils sont supplémentaires ! Par exemple, si $E = \mathcal{F}(\mathbb{R}, \mathbb{R})$, $F = \{f \in E \ / \ f(0) = 1\}$ et $G =< \cos >$, je vous laisse montrer que tout élément $f \in E$ s'écrit de façon unique $f = u + v$ avec $u \in F$ et $v \in G$, pourtant F et G ne sont supplémentaires dans E car F n'est pas un sous-espace vectoriel de E ;*
- *attention, si F est un sous-espace vectoriel de E, F admet en général une « infinité » de supplémentaires (en tout cas lorsque $\mathbb{K} \subset \mathbb{C}$). Par exemple, dans $\mathbb{R}^3$, si $\mathcal{P}$ est le plan vectoriel d'équation $z = 0$, alors $\mathbb{R}(0, 0, 1)$ est un supplémentaire de F dans $\mathbb{R}^3$, tout comme $\mathbb{R}(a, b, 1)$ pour tout $(a, b) \in \mathbb{R}^2$. Moralement, c'est assez simple à comprendre car pour un plan, on doit rajouter une direction pour obtenir tout l'espace, cette direction est quelconque mais ne doit pas être « dans le plan » ;*
- *enfin, une question naturelle est « un sous-espace vectoriel admet-il toujours au moins un supplémentaire » ? La réponse à cette question est en réalité assez compliquée : cela dépend de ce qu'on accepte comme axiomes sur les ensembles. Pour faire simple, la réponse est « ce n'est pas important ». Si l'existence d'un supplémentaire est nécessaire, il sera toujours précisé dans la pratique qu'on admet qu'il existe. Sinon, c'est qu'on n'en a pas besoin... Pour ceux qui sont curieux (et courageux), l'existence découle du lemme de Zorn qui est équivalent à l'axiome du choix mais ces notions dépassent de loin les objectifs de ce livre.*

4.2.4 Produit cartésien de deux espaces vectoriels

Proposition 4.2.4.1 *Soient E et F deux $\mathbb{K}$-espaces vectoriels. On munit $E \times F$ de deux lois :*

$$\forall (u,v),(u',v') \in E \times F \ , \ (u,v)+(u',v') = (u+u',v+v')$$

et

$$\forall \lambda \in \mathbb{K} \ , \ \forall (u,v) \in E \times F \ , \ \lambda \cdot (u,v) = (\lambda \cdot u, \lambda \cdot v)$$

Alors $(E \times F, +, \cdot)$ est un espace vectoriel.

Plus généralement, on peut faire de même avec un produit cartésien (fini).

Proposition 4.2.4.2 *Soient $n \geqslant 1$ et pour tout $i \in [\![1,n]\!]$, F_i un $\mathbb{K}$-espace vectoriel. On définit alors sur $E = \prod_{i=1}^{n} F_i$ une loi de composition interne $+$ et une loi de composition externe $\cdot$ respectivement définies par :*

$$\forall (u_1,\cdots,u_n) \in E, \ \forall (v_1,\cdots,v_n) \in E, \ (u_1,\cdots,u_n)+(v_1,\cdots,v_n) = (u_1+v_1,\cdots,u_n+v_n)$$

et

$$\forall (u_1,\cdots,u_n) \in E \ , \ \forall \lambda \in \mathbb{K} \ , \ \lambda \cdot (u_1,\cdots,u_n) = (\lambda \cdot u_1,\cdots,\lambda \cdot u_n)$$

Alors, $(E,+,\cdot)$ est un $\mathbb{K}$-espace vectoriel.

Preuve :

• Tout d'abord, $+$ est bien une loi de composition interne dans E et $\cdot$ est bien une loi de composition externe sur E.

• Montrons que $(E,+)$ est un groupe abélien.

∗ Montrons que $+$ est associative et commutative.
Soient $u = (u_1,\cdots,u_n)$, $v = (v_1,\cdots,v_n)$ et $w = (w_1,\cdots,w_n)$ trois éléments de E. On a :

$$\begin{aligned}(u+v)+w &= (u_1+v_1,\cdots,u_n+v_n)+(w_1,\cdots,w_n)\\ &= ((u_1+v_1)+w_1,\cdots,(u_n+v_n)+w_n)\\ &= (u_1+(v_1+w_1),\cdots,u_n+(v_n+w_n))\end{aligned}$$

car chaque F_i (pour $1 \leqslant i \leqslant n$) est un espace vectoriel donc l'addition dans F_i est associative. Par suite,

$$\begin{aligned}(u+v)+w &= (u_1,\cdots,u_n)+(v_1+w_1,\cdots,v_n+w_n)\\ &= u+(v+w)\end{aligned}$$

Ce qui prouve que $+$ est associative.
De plus, pour tout $i \in [\![1,n]\!]$, $(F_i,+)$ est un groupe abélien. Il est alors clair que $+$ est commutative.

∗ Montrons l'existence d'un neutre pour $+$.
On note pour $i \in [\![0,n]\!]$, 0_{F_i} le neutre de $(F_i,+)$. Il est alors évident que $0_E = (0_{F_1},\cdots,0_{F_n}) \in E$ est neutre pour $+$.

∗ Montrons que tout élément de E admet un opposé dans E.
Soit $u = (u_1,\cdots,u_n) \in E$. Alors $v = (-u_1,\cdots,-u_n) \in E$ vérifie $u+v = v+u = 0_E$.

Ce qui prouve que $(E,+)$ est un groupe abélien.

• Montrons à présent les propriétés $P1$, $P2$, $P3$ et $P4$. En réalité, ces propriétés sont évidentes car chaque F_i $(1 \leqslant i \leqslant n)$ est un $\mathbb{K}$-espace vectoriel, il vérifie donc chacun des axiomes $P1$, $P2$, $P3$ et $P4$ et il en est alors de même pour $(E,+,\cdot)$. Ceci étant dit, donnons néanmoins les détails pour certains de ces axiomes.

∗ Montrons $P1$.
Soient $(\lambda,\mu) \in \mathbb{K}^2$ et $u = (u_1,\cdots,u_n) \in E$. Alors :

$$\begin{aligned}(\lambda+\mu)\cdot u &= ((\lambda+\mu)\cdot u_1,\cdots,(\lambda+\mu)\cdot u_n)\\ &= (\lambda\cdot u_1+\mu\cdot u_1,\cdots,\lambda\cdot u_n+\mu\cdot u_n)\\ &= (\lambda\cdot u_1,\cdots,\lambda\cdot u_n)+(\mu\cdot u_1,\cdots,\mu\cdot u_n)\\ &= \lambda\cdot u+\mu\cdot v\end{aligned}$$

Les première et quatrième égalités proviennent de la définition de $\cdot$ dans E, la troisième provient de la définition de $+$ dans E et la seconde provient du fait que pour chaque $1 \leqslant i \leqslant n$, F_i est un espace vectoriel donc l'addition et la multiplication externe dans F_i vérifient la propriété $P1$.

∗ Les propriétés $P2$, $P3$ et $P4$ se démontrent de façon analogue. Je vous encourage à faire les preuves par vous-même.

⊠

Remarques : *il est important de remarquer les points suivants :*

- *tous les espaces vectoriels F_i sont des $\mathbb{K}$-espaces vectoriels pour le même corps $\mathbb{K}$! Sinon, on ne peut pas multiplier chaque composante par des scalaires dans $\mathbb{K}$.*
- *Dans la définition de l'addition dans $\prod_{i=1}^{n} F_i$, notez bien que l'addition de la i-ème*

composante se fait dans F_i. En toute rigueur, il faudrait écrire : $(F_i, +_i, \cdot_i)$ est un $\mathbb{K}$-espace vectoriel et dans ce cas,

$$(u_1, \cdots, u_n) + (v_1, \cdots, v_n) = (u_1 +_1 v_1, u_2 +_2 v_2, \cdots, u_n +_n v_n)$$

- *Les plus rigoureux d'entre vous ne seront pas d'accord avec la preuve précédente qui utilise des « $\cdots$ » et vous auriez raison ! Il faudrait en toute rigueur écrire « soit $u = (u_i)_{1 \leqslant i \leqslant n} \in E$ » et faire les calculs avec les éléments écrits sous cette forme. Je vous laisse le soin de le faire...*
- *Enfin, notez qu'on retrouve le fait que $\mathbb{K}^n$ est un $\mathbb{K}$-espace vectoriel (il suffit de choisir $F_i = \mathbb{K}$ pour tout $i \in [\![1, n]\!]$).*

4.3 Sous-espaces affines

4.3.1 Translations et groupes des translations d'un espace vectoriel

Définition 4.3.1.1 Soient E un espace vectoriel.

- Soit $u \in E$. On appelle translation de vecteur u l'application :

$$\begin{array}{rccc} t_u : & E & \longrightarrow & E \\ & x & \longmapsto & x + u \end{array}$$

- On dit qu'une application $T : E \longrightarrow E$ est une translation de E s'il existe $u \in E$ tel que $T = t_u$.

Proposition 4.3.1.2 *L'ensemble $\tau(E)$ des translations de E est un sous-groupe de $(\sigma(E), \circ)$, l'ensemble des bijections de E. De plus, ce groupe est isomorphe à $(E, +)$.*

Preuve :

On vérifie facilement (le faire) que pour tout $(u, v) \in E^2$:

$$(1) : \ \mathrm{Id}_E = t_{0_E} \qquad (2) : \ t_u \circ t_v = t_{u+v} \qquad (3) : \ t_{-u} = t_u^{-1}$$

En effet, d'après (1) et (2), $t_u \circ t_{-u} = t_{0_E} = \mathrm{Id}_E = t_{-u} \circ t_u$. Ce qui prouve que t_u est bijective et que sa bijection réciproque est t_{-u}.

- D'après ce que l'on vient de remarquer, $\tau(E) \subset \sigma(E)$.
- Ensuite,
  - ∗ d'après (1), $\mathrm{Id}_E \in \tau(E)$;
  - ∗ d'après (2), $\tau(E)$ est stable par composition ;
  - ∗ et d'après (3), $\tau(E)$ est stable par inverse.

Par conséquent, $\tau(E)$ est bien un sous-groupe de $(\sigma(E), \circ)$.

- Enfin, l'application $\varphi : \begin{array}{ccc} (E,+) & \longrightarrow & (\tau(E),\circ) \\ u & \longmapsto & t_u \end{array}$ est :
  - ∗ un morphisme de groupes d'après (2) ;
  - ∗ surjective par définition des translations ;
  - ∗ injective car :

$$\begin{aligned} \ker\varphi &= \{u \in E \ / \ t_u = \mathrm{Id}_E\} \\ &= \{u \in E \ / \ \forall x \in E \ , \ u + x = x\} \\ &= \{0_E\} \end{aligned}$$

Ce qui prouve que φ est bien un isomorphisme de groupes.

⊠

4.3.2 Définition d'un sous-espace affine

Définition 4.3.2.1 Soient E un $\mathbb{K}$-espace vectoriel et $\mathcal{A} \subset E$. On dit que $\mathcal{A}$ est un sous-espace affine de E s'il existe un sous-espace vectoriel F de E et un élément $u \in E$ tels que :

$$\mathcal{A} = t_u(F)$$

On a alors par définition,

$$a \in \mathcal{A} \iff \exists x \in F \ , \ a = u + x$$

et on note dans ce cas $\mathcal{A} = u + F$.

Remarques :

- *par définition, $0_E \in F$: il s'ensuit que $\mathcal{A}$ est forcément non vide et que $u \in \mathcal{A}$;*
- *E est un sous-espace affine de E puisque $E = t_{0_E}(E)$ et de même tout sous-espace vectoriel F de E est aussi un sous-espace affine de E car $F = t_{0_E}(F)$;*
- *soit $\mathcal{A}$ un sous-espace affine de E, en général :*
  - ∗ *les éléments de $\mathcal{A}$ sont appelés des points ;*
  - ∗ *les éléments de F sont en revanche des vecteurs.*

Exemple 4.3.2.2 Dans $\mathbb{R}^2$, l'ensemble $\mathcal{D} = \{(x, y) \in \mathbb{R}^2 \ / \ x + y = 1\}$ est un sous-espace affine de $\mathbb{R}^2$ mais n'est pas un sous-espace vectoriel. En effet,

- $(0, 0) \notin \mathcal{D}$ donc $\mathcal{D}$ n'est pas un sous-espace vectoriel ;
- si on note $\overrightarrow{\mathcal{D}} = \{(x, y) \in \mathbb{R}^2 \ / \ x + y = 0\} = \mathbb{R}(1, -1)$, alors $\overrightarrow{\mathcal{D}}$ est un sous-espace vectoriel de $\mathbb{R}^2$ et pour tout $(x, y) \in \mathbb{R}^2$,

$$(x, y) \in \mathcal{D} \iff (x - 1, y) \in \overrightarrow{\mathcal{D}} \iff (x, y) \in (1, 0) + \overrightarrow{\mathcal{D}}$$

Exemple 4.3.2.3 De même, dans $\mathbb{R}^3$, tout plan affine, c'est-à-dire tout ensemble $\mathcal{P}$ d'équation cartésienne $ax + by + cz = d$ avec $(a, b, c) \neq (0, 0, 0)$ et $d \in \mathbb{R}$ est un sous-espace affine de $\mathbb{R}^3$.
En effet, si on fixe un « point » (x_0, y_0, z_0) de ce plan $\mathcal{P}$, alors pour tout $(x, y, z) \in \mathbb{R}^3$:

$$(x, y, z) \in \mathcal{P} \iff (x - x_0, y - y_0, z - z_0) \in \overrightarrow{\mathcal{P}}$$

où $\overrightarrow{\mathcal{P}}$ est le plan « vectoriel » d'équation $ax + by + cz = 0$.

Exemple 4.3.2.4 L'ensemble $\mathcal{S}$ des solutions de $y'' + y = 2e^t$ est un sous-espace affine de $\mathcal{C}^0(\mathbb{R}, \mathbb{R})$. En effet,

$$\begin{aligned} y \in \mathcal{S} &\iff \exists (\lambda, \mu) \in \mathbb{R}^2 \ , \ \forall t \in \mathbb{R} \ , \ y(t) = e^t + \lambda \cos(t) + \mu \sin(t) \\ &\iff y - \exp \in < \cos, \sin > \\ &\iff y \in \exp + < \cos, \sin > \end{aligned}$$

Ainsi, $\mathcal{S} = \exp + < \cos, \sin >$ avec $\exp \in \mathcal{C}^0(\mathbb{R}, \mathbb{R})$ et $< \cos, \sin >$ un sous-espace vectoriel de $\mathcal{C}^0(\mathbb{R}, \mathbb{R})$.

Exercice 4.3.2.5 Montrer que l'ensemble des suites réelles $(u_n)_{n \in \mathbb{N}}$ vérifiant la relation de récurrence :

$$\forall n \in \mathbb{N} \ , \ u_{n+2} = 4u_{n+1} - 3u_n + 2^n$$

est un sous-espace affine de $\mathbb{R}^{\mathbb{N}}$.

Proposition 4.3.2.6 *Si $\mathcal{A} = u + F$ est un sous-espace affine de E, (avec F un sous-espace vectoriel de E et $u \in E$), alors :*

(i) F est unique. On dit que F est la direction du sous-espace affine $\mathcal{A}$ et on note $F = \overrightarrow{\mathcal{A}}$;

(ii) de plus, l'élément u peut être choisi arbitrairement dans $\mathcal{A}$, c'est-à-dire que :

$$\forall v \in \mathcal{A} \ , \ \mathcal{A} = v + \overrightarrow{\mathcal{A}}$$

Preuve :

• Montrons (i).
Supposons que $u+F = v+G$ où u, v sont deux vecteurs de E et F, G deux sous-espaces vectoriels de E. Montrons que $F \subset G$ pour commencer. Par symétries des rôles de F et G, on aura alors $F = G$.
Soit $x \in F$. Alors $u + x \in u + F$ et donc, compte-tenu de l'hypothèse, $u + x \in v + G$. Par définition, il existe alors $y \in G$ tel que :

$$u + x = v + y \quad \text{c'est-à-dire} \quad x = (v - u) + y = -(u - v) + y$$

Or, $0_E \in F$ (puisque F est un sous-espace vectoriel de E). On a donc :

$$u + 0_E \in v + G \quad \text{soit encore} \quad u - v \in G$$

Ainsi, $y \in G$, $u - v \in G$ et G est un sous-espace vectoriel de E. Par suite, $x = -(u - v) + y \in G$. D'où $F \subset G$.

• Montrons (ii).
On a déjà remarqué que si $\mathcal{A} = u + \overrightarrow{\mathcal{A}}$, alors $u \in \mathcal{A}$.
Montrons alors que si $(u, v) \in \mathcal{A}^2$, alors $\mathcal{A} = u + \overrightarrow{\mathcal{A}} = v + \overrightarrow{\mathcal{A}}$.
Soient u, v deux éléments quelconques de $\mathcal{A}$. D'après ce qui précède, il existe $x \in \overrightarrow{\mathcal{A}}$ tel que :

$$v = u + x$$

Alors, pour tout $y \in \overrightarrow{\mathcal{A}}$, $v + y = u + (x + y) \in u + \overrightarrow{\mathcal{A}}$, ce qui prouve que $v + \overrightarrow{\mathcal{A}} \subset u + \overrightarrow{\mathcal{A}}$.
Par symétrie des rôles de u et v, il y a alors égalité. ⊠

Remarque : *si $\mathcal{A}$ est un sous-espace affine de E, alors la direction de $\mathcal{A}$ est donnée par :*

$$\overrightarrow{\mathcal{A}} = \{x - y \ , \ (x, y) \in \mathcal{A}^2\}$$

Exercice 4.3.2.7 Soit $\mathcal{A}$ un sous-espace affine de E. À quelle condition, nécessaire et suffisante, $\mathcal{A}$ est-il un sous-espace vectoriel de E ?

Exercice 4.3.2.8 Déterminer la direction du plan P de l'espace défini par $x+2y+z = 3$.

Exercice 4.3.2.9 On note $\mathcal{S}$ l'ensemble des solutions de l'équation différentielle $ay'' + by'+cy = f(t)$ avec $(a, b, c) \in \mathbb{R}^3$ $(a \neq 0)$ et $f \in \mathcal{C}^0(\mathbb{R}, \mathbb{R})$. On rappelle qu'il existe toujours au moins une solution de cette équation.

1. Montrer que $\mathcal{S}$ est un sous-espace affine de $\mathcal{C}^0(\mathbb{R}, \mathbb{R})$.
2. Quelle est la direction de $\mathcal{S}$, c'est-à-dire déterminer $\overrightarrow{\mathcal{S}}$? *Il n'est pas nécessaire de savoir résoudre l'équation pour répondre à cette question.*

Proposition 4.3.2.10 *Si $\mathcal{A}$ et $\mathcal{B}$ sont des sous-espaces affines de E tels que $\mathcal{A} \subset \mathcal{B}$, alors $\overrightarrow{\mathcal{A}} \subset \overrightarrow{\mathcal{B}}$.*

Preuve :

Soit $u \in \mathcal{A}$. Alors $u \in \mathcal{B}$ et on a donc : $\mathcal{A} = u + \overrightarrow{\mathcal{A}}$ et $\mathcal{B} = u + \overrightarrow{\mathcal{B}}$.
Montrons que $\overrightarrow{\mathcal{A}} \subset \overrightarrow{\mathcal{B}}$.
Soit $x \in \overrightarrow{\mathcal{A}}$. Alors $u + x \in A \subset B$ donc $u + x \in u + \overrightarrow{\mathcal{B}}$. Par suite, $x \in \overrightarrow{\mathcal{B}}$.
⊠

4.3.3 Parallélisme

Définition 4.3.3.1 Soient E un $\mathbb{K}$-espace vectoriel, $\mathcal{A}$ et $\mathcal{B}$ deux sous-espaces affines de E. On dit que $\mathcal{A}$ est parallèle à $\mathcal{B}$ si $\overrightarrow{\mathcal{A}} \subset \overrightarrow{\mathcal{B}}$.

⚠ **Attention :** cette notion n'est pas du tout symétrique, contrairement à la notion de droites parallèles.

Exemple 4.3.3.2 On se place dans $\mathbb{R}^3$ et on note $(\vec{i}, \vec{j}, \vec{k})$ la base usuelle de $\mathbb{R}^3$. On considère la droite $\mathcal{D}$ de repère $(A; \vec{i})$ (autrement dit, $\mathcal{D} = A + \mathbb{R}(1, 0, 0)$), avec $A = (1, 1, 1)$ et le plan $\mathcal{P}$ d'équation cartésienne $y + z = 2$. Alors :

- la droite $\mathcal{D}$ est parallèle au plan $\mathcal{P}$ car :

$$\overrightarrow{\mathcal{D}} = \mathbb{R}\vec{i} \subset \mathrm{Vect}(\vec{i}, \vec{j} - \vec{k}) = \overrightarrow{\mathcal{P}}$$

- En revanche, il est faux de dire que le plan $\mathcal{P}$ est parallèle à la droite $\mathcal{D}$ puisque l'inclusion $\overrightarrow{\mathcal{P}} \subset \overrightarrow{\mathcal{D}}$ est fausse.

Définition 4.3.3.3 On dit que deux sous-espaces affines $\mathcal{A}$ et $\mathcal{B}$ d'un espace vectoriel E sont parallèles si $\mathcal{A}$ est parallèle à $\mathcal{B}$ et si $\mathcal{B}$ est parallèle à $\mathcal{A}$, c'est-à-dire si $\overrightarrow{\mathcal{A}} = \overrightarrow{\mathcal{B}}$. On note alors $\mathcal{A} \parallel \mathcal{B}$.

Exercice 4.3.3.4 Montrer que la relation $\parallel$ est une relation d'équivalence sur l'ensemble des sous-espaces affines de E.

4.3.4 Intersection de deux sous-espaces affines

Théorème 4.3.4.1 *Soient E un $\mathbb{K}$-ev, $\mathcal{A}$ et $\mathcal{B}$ deux sous-espaces affines de E. Alors $\mathcal{A} \cap \mathcal{B}$ est soit vide ou bien c'est un sous-espace affine de E de direction $\overrightarrow{\mathcal{A}} \cap \overrightarrow{\mathcal{B}}$.*

Preuve :

On suppose que $\mathcal{A} \cap \mathcal{B} \neq \emptyset$. Montrons que $\mathcal{A} \cap \mathcal{B}$ est un sous-espace affine de E de direction $\overrightarrow{\mathcal{A}} \cap \overrightarrow{\mathcal{B}}$.
Soit $u \in \mathcal{A} \cap \mathcal{B}$. On a alors :

$$\begin{aligned} x \in \mathcal{A} \cap \mathcal{B} &\iff x \in \mathcal{A} \text{ et } x \in \mathcal{B} \\ &\iff x - u \in \overrightarrow{\mathcal{A}} \text{ et } x - u \in \overrightarrow{\mathcal{B}} \\ &\iff x - u \in \overrightarrow{\mathcal{A}} \cap \overrightarrow{\mathcal{B}} \\ &\iff x \in u + \overrightarrow{\mathcal{A}} \cap \overrightarrow{\mathcal{B}} \end{aligned}$$

Ainsi, $\mathcal{A} \cap \mathcal{B} = u + \overrightarrow{\mathcal{A}} \cap \overrightarrow{\mathcal{B}}$. Or, $\overrightarrow{\mathcal{A}} \cap \overrightarrow{\mathcal{B}}$ est un sous-espace vectoriel de E (intersection de sous-espaces vectoriels) donc $\mathcal{A} \cap \mathcal{B}$ est un sous-espace affine de E de direction $\overrightarrow{\mathcal{A} \cap \mathcal{B}} = \overrightarrow{\mathcal{A}} \cap \overrightarrow{\mathcal{B}}$.

Pour terminer, il reste à justifier que le cas $A \cap B = \emptyset$ peut effectivement se produire. Par exemple, si $x, y \in E$ et $x \neq y$ (et donc $E \neq \{0\}$), alors $\{x\}$ et $\{y\}$ sont des sous-espaces affines de E dont l'intersection est vide.

⊠

Exercice 4.3.4.2 Justifier que pour tout $x \in E$, $\{x\}$ est un sous-espace affine de E. Peut-on généraliser cela à toute partie finie de E est un sous-espace affine de E ?

Remarque : *en fait cette proposition généralise ce que vous avez appris en géométrie dans l'espace et les règles d'incidence dans l'espace. Vous avez vu que l'intersection de deux plans $\mathcal{P}_1$ et $\mathcal{P}_2$ (non parallèles) est une droite et que cette droite est dirigée par un vecteur (non nul). Ce vecteur est justement un vecteur directeur de l'intersection $\overrightarrow{\mathcal{P}_1} \cap \overrightarrow{\mathcal{P}_2}$.*

En fait, la proposition précédente peut se généraliser à une intersection quelconque de sous-espaces affines.

Exercice 4.3.4.3 Soient E un $\mathbb{K}$-espace vectoriel et $(\mathcal{A}_i)_{i \in I}$ une famille quelconque de sous-espaces affines de E. Montrer que $\bigcap_{i \in I} \mathcal{A}_i$ est soit vide, soit un sous-espace affine de direction $\bigcap_{i \in I} \overrightarrow{\mathcal{A}_i}$.

4.4 Applications linéaires

4.4.1 Définition et exemples

Définition 4.4.1.1 Soient E et F deux $\mathbb{K}$-espaces vectoriels. On dit qu'une application $f : E \longrightarrow F$ est linéaire, ou encore un morphisme de $\mathbb{K}$-espaces vectoriels, si elle vérifie :

(i) $\forall x, y \in E$, $f(x+y) = f(x) + f(y)$
(ii) $\forall x \in E$, $\forall \lambda \in \mathbb{K}$, $f(\lambda \cdot x) = \lambda \cdot f(x)$

Exemple 4.4.1.2 L'application dérivation $D : \begin{array}{ccc} \mathcal{C}^1 & \longrightarrow & \mathcal{C}^0 \\ f & \longmapsto & f' \end{array}$ est une application linéaire car :

$$\forall (f,g) \in \mathcal{C}^1(\mathbb{R},\mathbb{R})^2 \ , \ D(f+g) = (f+g)' = f' + g' = D(f) + D(g)$$

et

$$\forall f \in \mathcal{C}^1(\mathbb{R},\mathbb{R}) \ , \ \forall \lambda \in \mathbb{R} \ , \ D(\lambda f) = (\lambda f)' = \lambda f' = \lambda D(f)$$

Exemple 4.4.1.3 L'application f définie par : $\forall (x,y) \in \mathbb{R}^2$, $f(x,y) = (x+y, x-y)$ est une application linéaire de $\mathbb{R}^2$ dans $\mathbb{R}^2$. En effet,

- Pour tous $(x,y), (x',y') \in \mathbb{R}^2$,

$$\begin{array}{rcl} f((x,y)+(x',y')) & = & f(x+x', y+y') \\ & = & ((x+x')+(y+y'), (x+x')-(y+y')) \\ & = & ((x+y)+(x'+y'), (x-y)+(x'-y')) \\ & = & (x+y, x-y)+(x'+y', x'-y') \\ & = & f(x,y)+f(x',y') \end{array}$$

- Pour tout $(x,y) \in \mathbb{R}^2$ et tout $\lambda \in \mathbb{R}$,

$$\begin{array}{rcl} f(\lambda(x,y)) & = & f(\lambda x, \lambda y) \\ & = & (\lambda x + \lambda y, \lambda x - \lambda y) \\ & = & (\lambda(x+y), \lambda(x-y)) \\ & = & \lambda(x+y, x-y) \\ & = & \lambda f(x,y) \end{array}$$

⚠ **Attention :** première chose, il s'agit d'espaces vectoriels sur un même corps $\mathbb{K}$! Deuxième chose, dans certains cas, il est nécessaire de préciser s'il s'agit d'une application

$\mathbb{R}$-linéaire ou $\mathbb{C}$-linéaire, c'est-à-dire de préciser si on considère les espaces comme des $\mathbb{R}$-ev ou des $\mathbb{C}$-ev.

Exemple 4.4.1.4 On considère $E = \mathbb{C}$ et c la conjugaison complexe, c'est-à-dire $z \longmapsto \bar{z}$.

- Si on considère E en tant que $\mathbb{R}$-espace vectoriel, alors c est une application linéaire car :
$$\forall (z, z') \in \mathbb{C}^2 \ , \ \overline{z + z'} = \overline{z} + \overline{z'}$$
et
$$\forall z \in \mathbb{C} \ , \ \forall \lambda \in \mathbb{R} \ , \ \overline{\lambda z} = \overline{\lambda} \times \overline{z} = \lambda \times \overline{z} = \lambda \overline{z}$$
- En revanche, si on considère $E = \mathbb{C}$ en tant que $\mathbb{C}$-espace vectoriel, la conjugaison n'est pas une application linéaire car, par exemple :
$$\overline{i \cdot 1_{\mathbb{C}}} = \overline{i} = -i \neq i = i \cdot \overline{1_{\mathbb{C}}}$$

La conjugaison est donc une application $\mathbb{R}$-linéaire mais n'est pas $\mathbb{C}$-linéaire.

Exemple 4.4.1.5 On se place dans $E = \mathbb{R}^3$ et on fixe un vecteur $v \in \mathbb{R}^3$. Alors l'application :
$$f : \begin{array}{ccc} \mathbb{R}^3 & \longrightarrow & \mathbb{R}^3 \\ u & \longmapsto & u \wedge v \end{array}$$
est une application linéaire (propriété connue du produit vectoriel). Par contre, si on choisit $E = \mathbb{R}^3 \times \mathbb{R}^3$ (qui est un espace vectoriel car c'est un produit cartésien d'espaces vectoriels) et on considère :
$$\varphi : \begin{array}{ccc} \mathbb{R}^3 \times \mathbb{R}^3 & \longrightarrow & \mathbb{R}^3 \\ (u, v) & \longmapsto & u \wedge v \end{array}$$
φ est « bilinéaire », c'est-à-dire linéaire à droite et à gauche (on reverra cela un peu plus loin) mais φ n'est pas une application linéaire car par exemple,
$$\varphi(2\vec{i}, 2\vec{j}) = (2\vec{i}) \wedge (2\vec{j}) = 4(\vec{i} \wedge \vec{j}) = 4\vec{k} \neq 2\vec{k} = 2(\vec{i} \wedge \vec{j}) = 2\varphi(\vec{i}, \vec{j})$$

Exemple 4.4.1.6 Soit Ω un univers fini non vide et soit $E = \mathcal{F}(\Omega, \mathbb{R})$ l'ensemble des variables aléatoires réelles sur Ω. Alors :

- l'application $\mathbb{E}$ qui à $X \in E$ associe l'espérance de X, notée $\mathbb{E}(X)$, est une application linéaire de E dans $\mathbb{R}$;
- l'application $\mathbb{V}$ qui à $X \in E$ associe la variance de X, notée $\mathbb{V}(X)$, n'est pas linéaire.

Exercice 4.4.1.7 On suppose ici que $\mathbb{K} = \mathbb{Q}$ et $E = \mathbb{R}$ (autrement dit, on considère $\mathbb{R}$ en tant que $\mathbb{Q}$-espace vectoriel). On note f l'application définie par :

$$\forall x \in \mathbb{R}\ ,\ f(x) = \begin{cases} x & \text{si } x \in \mathbb{Q} \\ 0 & \text{sinon} \end{cases}$$

1. Montrer que : $\forall x \in \mathbb{R}\ ,\ \forall \lambda \in \mathbb{Q}\ ,\ f(\lambda \cdot x) = \lambda \cdot f(x)$.
2. f est-elle une application $\mathbb{Q}$-linéaire de $\mathbb{R}$ dans $\mathbb{R}$?

Remarque : *dans les exemples (et l'exercice) précédents, on a montré que les conditions (i) et (ii) de la définition d'une application linéaire sont « indépendantes », c'est-à-dire qu'une application peut vérifier (i) mais pas (ii), ou bien (ii) mais pas (i), ou bien ni l'une ni l'autre.*

Exercice 4.4.1.8 Soit $f : \mathbb{R} \longrightarrow \mathbb{R}$.

1. On suppose qu'il existe $a \in \mathbb{R}$ tel que : $\forall x \in \mathbb{R}\ ,\ f(x) = ax$. Montrer que f est $\mathbb{R}$-linéaire.
2. Montrer la réciproque.

Exercice 4.4.1.9 Soit E l'ensemble des fonctions $2T$-périodiques de $\mathbb{R}$ dans $\mathbb{R}$. Pour $a \in \mathbb{R}$, on considère l'application :

$$\varphi_a : \begin{array}{ccc} E & \longrightarrow & E \\ f & \longmapsto & (x \longmapsto f(x+a)) \end{array}$$

1. L'application φ_a est-elle bien définie ? Est-elle linéaire ?
2. L'application $\varphi : a \longmapsto \varphi_a$ est-elle linéaire ?

Si f est une application linéaire de E dans F, alors, en particulier, f est un morphisme de groupes de $(E, +)$ dans $(F, +)$. Il s'ensuit la proposition suivante déjà établie dans le chapitre sur les groupes.

Proposition 4.4.1.10 *Si f est linéaire de E dans F, alors :*

$$f(0_E) = 0_F \quad \text{et} \quad \forall x \in E\ ,\ f(-x) = -f(x)$$

Proposition 4.4.1.11 *Soient E et F deux $\mathbb{K}$-espaces vectoriels et soit f une application de E dans F. Alors les énoncés suivants sont équivalents :*

(i) *f est une application linéaire ;*
(ii) $\forall (x,y) \in E^2$, $\forall (\lambda,\mu) \in \mathbb{K}^2$, $f(\lambda \cdot x + \mu \cdot y) = \lambda \cdot f(x) + \mu \cdot f(y)$;
(iii) $\forall (x,y) \in E^2$, $\forall \lambda \in \mathbb{K}$, $f(\lambda \cdot x + y) = \lambda \cdot f(x) + f(y)$.

Preuve :

• Montrons $(i) \Longrightarrow (ii)$.
On suppose que f est linéaire. Soient $(x,y) \in E^2$ et $(\lambda,\mu) \in \mathbb{K}^2$. Alors :

$$\begin{array}{rcll} f(\lambda \cdot x + \mu \cdot y) & = & f(\lambda \cdot x) + f(\mu \cdot y) & \text{(propriété 1 de « linéaire »)} \\ & = & \lambda \cdot f(x) + \mu \cdot f(y) & \text{(propriété 2 de « linéaire »)} \end{array}$$

• L'implication $(ii) \Longrightarrow (iii)$ est évidente car il suffit de choisir $\mu = 1_{\mathbb{K}}$ (et on sait que pour $y \in E$, $1_{\mathbb{K}} \cdot y = y$ et $1_{\mathbb{K}} \cdot f(y) = f(y)$).

• L'implication $(iii) \Longrightarrow (i)$ est elle aussi évidente car :

∗ en choisissant $\lambda = 1_{\mathbb{K}}$ (dans (iii)), on obtient la première propriété de la définition d'une application linéaire ;

∗ en choisissant $y = 0_E$ (dans (iii)), on obtient la seconde.

⊠

Exercice 4.4.1.12 Pour $(a,b,c) \in \mathbb{C}^3$, l'application φ : $\begin{array}{rcl} \mathcal{C}^2(\mathbb{R},\mathbb{C}) & \longrightarrow & \mathcal{C}^0(\mathbb{R},\mathbb{C}) \\ y & \longmapsto & ay'' + by' + cy \end{array}$ est-elle une application $\mathbb{C}$-linéaire ?

Exercice 4.4.1.13 Montrer que l'application de $\mathbb{R}^{\mathbb{N}}$ dans lui-même qui à une suite (u_n) associe la suite $(u_{n+1} - u_n)$ est une application linéaire.

Définition 4.4.1.14 Une application linéaire de E dans $\mathbb{K}$ est appelée une forme linéaire (sur E).

Exemple 4.4.1.15 Si $\vec{u}$ est un vecteur fixé de l'espace, l'application $f : \mathbb{R}^3 \longrightarrow \mathbb{R}$ définie par $\forall \vec{x} \in \mathbb{R}^3$, $f(\vec{x}) = \vec{u} \cdot \vec{x} = (\vec{u}|\vec{x})$ (le produit scalaire usuel) est une forme linéaire.

Exemple 4.4.1.16 L'application de l'ensemble E des suites réelles convergentes dans $\mathbb{R}$ qui à une suite convergente $(u_n)_{n\in\mathbb{N}}$ associe sa limite est une forme linéaire (opérations algébriques sur les suites convergentes).

Exemple 4.4.1.17 $\varphi : \begin{array}{ccc} \mathcal{C}^0([0,1],\mathbb{R}) & \longrightarrow & \mathbb{R} \\ f & \longmapsto & \displaystyle\int_0^1 f(x)\,\mathrm{d}x \end{array}$ est une forme linéaire.

Exemple 4.4.1.18 En revanche, l'application qui à $(x,y)\in\mathbb{R}^2$ associe sa norme usuelle, c'est-à-dire $\sqrt{x^2+y^2} = \|(x,y)\|$, est une application de $\mathbb{R}^2$ dans $\mathbb{R}$, mais ce n'est pas une forme linéaire sur $\mathbb{R}^2$ (car par exemple $\|-1\cdot(1,0)\| = \|(1,0)\| \neq -\|(1,0)\|$).

Exercice 4.4.1.19 Montrer que les évaluations sont des formes linéaires. Autrement dit, montrer que si X est un ensemble non vide quelconque et $E = \mathcal{F}(X,\mathbb{R})$, alors pour tout $a\in X$, l'application $f\longmapsto f(a)$ est une forme linéaire sur $E=\mathcal{F}(X,\mathbb{R})$.

Notations et vocabulaire :

- on note $\mathcal{L}_{\mathbb{K}}(E,F)$ l'ensemble des applications $\mathbb{K}$-linéaires de E dans F. S'il n'y a pas de risques de confusions, on le note aussi $\mathcal{L}(E,F)$;
- si E est un $\mathbb{K}$-espace vectoriel, on note $\mathcal{L}_{\mathbb{K}}(E)$ l'ensemble des applications $\mathbb{K}$-linéaires de E dans E. S'il n'y a pas de risques de confusions, on le note aussi $\mathcal{L}(E)$;
- si E est un $\mathbb{K}$-espace vectoriel, l'ensemble des formes linéaires sur E est appelé l'espace dual de E (ou le dual algébrique de E). On note en général $E^\star = \mathcal{L}_{\mathbb{K}}(E,\mathbb{K})$.

4.4.2 Noyau et image d'une application linéaire

Définition 4.4.2.1 Soit $f\in\mathcal{L}(E,F)$. On définit :

- le noyau de f, noté $\ker(f)$, par $\ker(f) = \{x\in E \ / \ f(x)=0_F\} = f^{-1}(\{0_F\})$;
- l'image de f, notée $\mathrm{Im}(f)$, par $\mathrm{Im}f = \{y\in F \ / \ \exists x\in E\ ,\ y=f(x)\}$.

⚠ **Attention :** je vous rappelle que $f^{-1}(\{0_F\})$ est l'image réciproque de $\{0_F\}$ par f. Cette image réciproque est toujours définie et cette écriture ne suppose pas du tout que f est bijective !

Théorème 4.4.2.2 *Soient E et F deux $\mathbb{K}$-espaces vectoriels et soit f une application linéaire de E dans F.*

(i) $\ker(f)$ *est un sous-espace vectoriel de* E *;*

(ii) $\mathrm{Im}(f)$ *est un sous-espace vectoriel de* F *;*

(ii) f *est injective si et seulement si* $\ker(f) = \{0_E\}$ *;*

(iii) f *est surjective si et seulement si* $\mathrm{Im}(f) = F$.

Preuve :

• Montrons (i).
Puisque $f \in \mathcal{L}(E,F)$, f est aussi un morphisme de groupes de $(E,+)$ dans $(F,+)$. On en déduit donc que $(\ker(f),+)$ est un sous-groupe de $(E,+)$. En particulier,

* $0_E \in \ker(f)$;
* $\forall (x,x') \in (\ker(f))^2$, $x + x' \in \ker(f)$.

Par ailleurs, si $x \in \ker(f)$ et $\lambda \in \mathbb{K}$, $f(\lambda \cdot x) = \lambda \cdot f(x) = \lambda \cdot 0_F = 0_F$. Ce qui prouve que $\lambda \cdot x \in \ker(f)$ et montre donc, avec les deux points précédents, que $\ker(f)$ est un sous-espace vectoriel de E.

• La démonstration de (ii) est identique (et laissée en exercice).

• Montrons (iii).
On a déjà remarqué qu'une application linéaire est en particulier un morphisme de groupes. Par suite, f est injective si et seulement si $\ker(f) = \{0_E\}$.

• La propriété (iv) est vraie pour toute application, linéaire ou non !

⊠

Exemple 4.4.2.3 Soit $f : \mathbb{R}^3 \longrightarrow \mathbb{R}^2$ définie par $f((x,y,z)) = (x+z, x-y)$.

- Montrons que f est une application linéaire.
  Soient $u = (x,y,z)$, $v = (x',y',z')$ deux éléments de $\mathbb{R}^3$ et λ, μ deux réels.

$$\begin{aligned} f(\lambda \cdot u + \mu \cdot v) &= f((\lambda x + \mu x', \lambda y + \mu y', \lambda z + \mu z')) \\ &= ((\lambda x + \mu x') + (\lambda z + \mu z'), (\lambda x + \mu x') - (\lambda y + \mu y')) \\ &= (\lambda(x+z) + \mu(x'+z'), \lambda(x-y) + \mu(x'-y')) \\ &= (\lambda(x+z), \lambda(x-y)) + (\mu(x'+z'), \mu(x'-y')) \\ &= \lambda \cdot (x+z, x-y) + \mu \cdot (x'+z', x'-y') \\ &= \lambda \cdot f(u) + \mu \cdot f(v) \end{aligned}$$

Ce qui prouve que $f \in \mathcal{L}(\mathbb{R}^3, \mathbb{R}^2)$.

- Déterminons le noyau de f.
  Soit $(x, y, z) \in \mathbb{R}^3$.

$$\begin{array}{rcl}(x,y,z) \in \ker(f) & \iff & f(x,y,z) = 0 \\ & \iff & \left\{ \begin{array}{rcl} 0 & = & x+z \\ 0 & = & x-y \end{array} \right. \\ & \iff & \left\{ \begin{array}{rcl} y & = & x \\ z & = & -x \end{array} \right. \\ & \iff & (x,y,z) = x(1,1,-1) \\ & \iff & (x,y,z) \in \mathrm{Vect}((1,1,-1)) \end{array}$$

  Ainsi, $\ker(f) = \mathbb{R}(1,1,-1)$. On en déduit donc que f n'est pas injective car $\ker(f) \neq \{0_{\mathbb{R}^3}\}$.

- Déterminons l'image de f.

  Soit $(a, b) \in \mathbb{R}^2$ et soit $(x, y, z) \in \mathbb{R}^3$.

$$\begin{array}{rcl} f(x,y,z) = (a,b) & \iff & \left\{ \begin{array}{rcl} a & = & x+z \\ b & = & x-y \end{array} \right. \\ & \iff & \left\{ \begin{array}{rcl} z & = & a-x \\ y & = & b+x \end{array} \right. \\ & \iff & (x,y,z) = (x, b+x, a-x) \end{array}$$

  Ainsi, on a montré que pour tout $(a, b) \in \mathbb{R}^2$, l'équation $f(x, y, z) = (a, b)$ admet toujours une solution (en fait une infinité ici). Ce qui prouve que $\mathrm{Im}(f) = \mathbb{R}^2$ et f est donc surjective.

Remarque : *on pouvait aussi montrer que :*

$$\begin{array}{rcl} \mathrm{Im}(f) & = & < f(1,0,0), f(0,1,0), f(0,0,1) > \\ & = & < (1,1), (0,-1), (1,0) > \\ & = & < (1,0), (0,1) > \\ & = & \mathbb{R}^2 \end{array}$$

On reverra cela dans le cours de mathématiques supérieures 2, lorsqu'on étudiera de façon plus formelle la notion de base.

Exercice 4.4.2.4 Soit $\overrightarrow{\mathcal{E}}$ l'espace habituel et soit $\vec{u} \in \overrightarrow{\mathcal{E}}$ un vecteur de l'espace. On a déjà vu que $f(\vec{x}) = \vec{u} \cdot \vec{x}$ est une forme linéaire.

1. Son noyau est donc un sous-espace vectoriel de $\overrightarrow{\mathcal{E}}$: quel résultat retrouve-t-on ainsi ?
2. Quelle est l'image de f ?

Exemple 4.4.2.5 On considère $E = \mathcal{C}^0([0,1],\mathbb{R})$ et l'application $\varphi : E \longrightarrow E$ définie par :

$$\forall f \in E \ , \ \forall x \in [0,1] \ , \ \varphi(f)(x) = f(x) - \int_0^x f(t)\,\mathrm{d}t$$

Montrons que φ est linéaire et déterminons son noyau et son image.

- Tout d'abord, on peut commencer par remarquer que φ est bien une application. En effet, si f est continue sur $[0,1]$, alors d'après le théorème fondamental de l'analyse [2], $F : x \longmapsto \displaystyle\int_0^x f(t)\,\mathrm{d}t$ est une primitive de f. Cette fonction est dérivable (de dérivée f) et *a fortiori*, est continue. Il s'ensuit que $\varphi(f) = f - F$ est continue sur $[0,1]$, c'est-à-dire $\varphi(f) \in E$.
- De plus, d'après le cours, E est un $\mathbb{R}$-espace vectoriel. Montrons alors que φ est bien une application linéaire.
  Soient $(f,g) \in E^2$ et $(\lambda,\mu) \in \mathbb{R}^2$. On veut montrer que :
  $$\varphi(\lambda \cdot f + \mu \cdot g) = \lambda \cdot \varphi(f) + \mu \cdot \varphi(g)$$
  Il s'agit d'une égalité dans E (donc une égalité entre applications). On veut donc prouver que :
  $$\forall x \in [0,1] \ , \ \varphi(\lambda \cdot f + \mu \cdot g)(x) = (\lambda \cdot \varphi(f) + \mu \cdot \varphi(g))\,(x) = \lambda\varphi(f)(x) + \mu \cdot \varphi(g)(x)$$
  Soit $x \in [0,1]$. Par définition de l'addition de fonctions et par linéarité de l'intégrale, on a :
  $$\begin{aligned}
  \varphi(\lambda \cdot f + \mu \cdot g)(x) &= (\lambda \cdot f + \mu \cdot g)(x) - \int_0^x (\lambda \cdot f + \mu \cdot g)(t)\,\mathrm{d}t \\
  &= \lambda f(x) + \mu g(x) - \int_0^x (\lambda \cdot f(t) + \mu \cdot g(t))\,\mathrm{d}t \\
  &= \lambda f(x) + \mu g(x) - \lambda \int_0^x f(t)\,\mathrm{d}t - \mu \int_0^x g(t)\,\mathrm{d}t \\
  &= \lambda \left(f(x) - \int_0^x f(t)\,\mathrm{d}t \right) + \mu \left(g(x) - \int_0^x g(t)\,\mathrm{d}t \right) \\
  &= \lambda\varphi(f)(x) + \mu\varphi(g)(x)
  \end{aligned}$$
  Ceci étant vrai pour tout réel $x \in [0,1]$, on a bien :
  $$\varphi(\lambda \cdot f + \mu \cdot g) = \lambda \cdot \varphi(f) + \mu \cdot \varphi(g)$$
  Ce qui prouve que φ est linéaire.

2. voir cours de mathématiques supérieures 2.

- Déterminons alors le noyau de φ.
  Soit $f \in E$. Par définition,

$$f \in \ker(\varphi) \iff \forall x \in [0,1]\ ,\ f(x) - \int_0^x f(t)\,\mathrm{d}t = 0$$

  Notons $F : x \longmapsto \displaystyle\int_0^x f(t)\,\mathrm{d}t$. Alors, F est la primitive de f qui s'annule en 0 et par suite,

$$\begin{aligned} f \in \ker(\varphi) &\iff \left\{ \begin{array}{l} -F + f = 0 \\ F(0) = 0 \end{array} \right. \\ &\iff \left\{ \begin{array}{l} F' - F = 0 \\ F(0) = 0 \end{array} \right. \\ &\iff F = 0 \\ &\iff f = 0 \end{aligned}$$

  Ce qui prouve que $\ker(\varphi) = \{0_E\}$ et donc φ est injective.

  Remarque : *si l'utilisation des équivalences pose problème (c'est-à-dire si vous n'êtes pas certain que vos équivalences sont des équivalences), il vaut mieux rédiger par analyse-synthèse. Ici, dans l'analyse, on obtient $F' - F = 0$ donc $F = \lambda \exp$ avec $\lambda \in \mathbb{R}$. Or, $F(0) = 0$ donc $\lambda = 0$ et $F = 0$. Par suite, $f = F' = 0$. Dans cet exemple, l'inclusion réciproque (c'est-à-dire la synthèse) est inutile car $0_E \in \ker(\varphi)$.*

- Déterminons à présent l'image de φ.

  Soient $g \in E$ et $f \in E$. En conservant les mêmes notations que juste avant, on a :

$$\varphi(f) = g \iff \left\{ \begin{array}{l} -F' + F = g \\ F(0) = 0 \end{array} \right.$$

  Or, g est continue sur $[0,1]$ donc d'après le cours sur les équations différentielles linéaires d'ordre 1, l'équation différentielle $-y' + y = g$ admet une unique solution qui vérifie $y(0) = 0$. Alors $f = y'$ est solution de $\varphi(f) = g$ (et c'est la seule).
  Ce qui prouve que $\mathrm{Im}(\varphi) = E$ et φ est donc surjective.

Remarque : *dans cet exemple, on aurait directement pu montrer que φ est bijective en utilisant le raisonnement pour déterminer les antécédents de g. C'est plus rapide mais cela suppose déjà que l'on sait que φ est bijective. Ceci est d'autant plus délicat qu'en général, déterminer le noyau est bien plus simple que de trouver l'image.*

Exercice 4.4.2.6 Soit $\vec{v} \in \overrightarrow{\mathcal{E}}$. Déterminer le noyau et l'image de $\vec{u} \longmapsto \vec{u} \wedge \vec{v}$.

Exercice 4.4.2.7 Soit $E = \{(u_n)_{n\in\mathbb{N}} \in \mathbb{R}^{\mathbb{N}} \ / \ (u_n)_{n\in\mathbb{N}} \text{ converge } \}$. On note f l'application définie par :

$$\forall (u_n)_{n\in\mathbb{N}} \in E \ , \ f((u_n)_{n\in\mathbb{N}}) = (u_{n+1} - u_n)_{n\in\mathbb{N}}$$

On sait que f est linéaire (voir l'exercice 4.4.1.13). Déterminer le noyau et l'image de f.

▶ Méthode :

Pour montrer que F est un espace vectoriel, on peut :

1. montrer que c'est un sous-espace vectoriel d'un espace vectoriel connu ;
2. montrer que c'est le noyau d'une application linéaire ;
3. montrer que c'est l'image d'une application linéaire ;
4. montrer que c'est un produit cartésien ou une intersection d'espaces vectoriels connus ;
5. revenir à la définition d'un espace vectoriel.

4.4.3 Équations linéaires

Définition 4.4.3.1 Soient E et F des espaces vectoriels. On dit qu'une équation $(\mathcal{E})$ d'inconnue $x \in E$ est linéaire s'il existe $\varphi \in \mathcal{L}(E, F)$ et $b \in F$ tels que :

$$x \text{ est solution de l'équation } (\mathcal{E}) \iff \varphi(x) = b$$

Exemple 4.4.3.2 Soit $\vec{u} \in \overrightarrow{\mathcal{E}}$. L'équation dans $\overrightarrow{\mathcal{E}}$, $\vec{x} \wedge \vec{u} = \vec{v}$ est une équation linéaire.

Exemple 4.4.3.3 Les équations différentielles linéaires du premier et du second ordre sont des équations linéaires.

Exemple 4.4.3.4 L'équation $(\mathcal{E})$ dans $\mathbb{R}^{\mathbb{N}}$: $\forall n \in \mathbb{N}$, $au_{n+2} + bu_{n+1} + cu_n = d_n$, où $(a, b, c) \in \mathbb{R}^3$ et $(d_n)_{n\in\mathbb{N}} \in \mathbb{R}^{\mathbb{N}}$ sont donnés est une équation linéaire.

Exemple 4.4.3.5 En revanche, l'équation : $y' = 1 + y^2$ dans $E = \mathcal{C}^1$ n'est pas une équation linéaire.

Proposition 4.4.3.6 *Si $(\mathcal{E})$ est une équation linéaire, alors l'ensemble $\mathcal{S}$ des solutions de $(\mathcal{E})$ est soit vide soit un sous-espace affine de E, de direction* $\ker(\varphi)$.

Preuve :

Si $\mathcal{S} \neq \emptyset$, on choisit $x_0 \in \mathcal{S}$. Alors, pour tout $x \in E$,

$$\varphi(x) = b \iff \varphi(x) = \varphi(x_0) \iff \varphi(x - x_0) = 0$$

c'est-à-dire $\varphi(x) = b \iff x - x_0 \in \ker(\varphi)$. D'où $\mathcal{S} = x_0 + \ker(\varphi)$. ⊠

4.4.4 Ensembles des applications linéaires $\mathcal{L}(E, F)$

Proposition 4.4.4.1 *Soient E et F deux $\mathbb{K}$-espaces vectoriels. Alors, l'ensemble $\mathcal{L}_{\mathbb{K}}(E, F)$ est un sous-espace vectoriel de $\mathcal{F}(E, F)$.*

Preuve :

• Pour commencer, on peut noter que $\mathcal{L}_{\mathbb{K}}(E, F) \subset \mathcal{F}(E, F)$.

• L'application nulle de E dans F, c'est-à-dire $0_{\mathcal{F}(E,F)}$ est une application linéaire puisque pour tout $(x, y) \in E^2$ et tout $(\lambda, \mu) \in \mathbb{K}^2$:

$$\begin{aligned} 0_{\mathcal{F}(E,F)}(\lambda \cdot x + \mu \cdot y) &= 0_F \\ &= \lambda \cdot 0_F + \mu \cdot 0_F \\ &= \lambda 0_{\mathcal{F}(E,F)}(x) + \mu 0_{\mathcal{F}(E,F)}(y) \end{aligned}$$

• Stabilité par combinaisons linéaires.
Soient $f, g \in \mathcal{L}_{\mathbb{K}}(E, F)$ et $\lambda, \mu \in \mathbb{K}$. Montrons que $h = \lambda \cdot f + \mu \cdot g$ est une application linéaire. Soient $x, y \in E$ et $\alpha \in \mathbb{K}$. On a alors :

$$\begin{aligned} h(\alpha \cdot x + y) &= (\lambda \cdot f + \mu \cdot g)(\alpha \cdot x + y) \\ &= \lambda \cdot f(\alpha x + y) + \mu \cdot g(\alpha x + y) \\ &= \lambda \cdot (\alpha \cdot f(x) + f(y)) + \mu \cdot (\alpha \cdot g(x) + g(y)) \end{aligned}$$

puisque f, g sont linéaires. On a ainsi :

$$\begin{aligned} h(\alpha \cdot x + y) &= (\lambda \times \alpha) \cdot f(x) + \lambda \cdot f(y) + (\mu \times \alpha) \cdot g(x) + \mu \cdot g(y) \\ &= (\alpha \times \lambda) \cdot f(x) + \lambda \cdot f(y) + (\alpha \times \mu) \cdot g(x) + \mu \cdot g(y) \end{aligned}$$

car $\mathbb{K}$ est un corps commutatif. Enfin, en groupant les termes, on obtient :

$$\begin{aligned} h(\alpha \cdot x + y) &= \alpha \cdot (\lambda \cdot f(x) + \mu \cdot g(x)) + \lambda \cdot f(y) + \mu \cdot g(y) \\ &= \alpha \cdot h(x) + h(y) \end{aligned}$$

Ce qui prouve que h est linéaire, *i.e.* $\lambda \cdot f + \mu \cdot g \in \mathcal{L}_{\mathbb{K}}(E, F)$. ⊠

Définition 4.4.4.2 Lorsque $F = E$, l'ensemble $\mathcal{L}_{\mathbb{K}}(E,F)$ est noté $\mathcal{L}_{\mathbb{K}}(E)$ (ou tout simplement $\mathcal{L}(E)$ s'il n'y a pas de risque de confusion). Un élément de $\mathcal{L}(E)$ est appelé un endomorphisme de E.

Théorème 4.4.4.3 *Soient E, F et G trois $\mathbb{K}$-espaces vectoriels.*

1. Soient $f \in \mathcal{L}(E,F)$ et $g \in \mathcal{L}(F,G)$.

(i) $g \circ f \in \mathcal{L}(E,G)$. En clair, lorsque cela a un sens, la composée d'applications linéaires est encore linéaire.

(ii) $g \circ f = 0$ si et seulement si $\mathrm{Im} f \subset \ker g$.

2. L'application $\varphi : \begin{array}{ccc} \mathcal{L}(F,G) \times \mathcal{L}(E,F) & \longrightarrow & \mathcal{L}(E,G) \\ (g,f) & \longmapsto & g \circ f \end{array}$ *est bilinéaire, c'est-à-dire :*

$$\forall g \in \mathcal{L}(F,G)\ ,\ \forall f_1, f_2 \in \mathcal{L}(E,F)\ ,\ \forall \lambda \in \mathbb{K}\ ,\ g \circ (\lambda \cdot f_1 + f_2) = \lambda \cdot (g \circ f_1) + g \circ f_2$$

$$\forall f \in \mathcal{L}(E,F)\ ,\ \forall g_1, g_2 \in \mathcal{L}(F,G)\ ,\ \forall \lambda \in \mathbb{K}\ ,\ (\lambda \cdot g_1 + g_2) \circ f = \lambda \cdot (g_1 \circ f) + g_2 \circ f$$

Preuve :

• Montrons 1. Soient $f \in \mathcal{L}_{\mathbb{K}}(E,F)$ et $g \in \mathcal{L}_{\mathbb{K}}(F,G)$.

(i) Soient $x, y \in E$ et $\lambda \in \mathbb{K}$. Alors, en utilisant successivement la linéarité de f puis celle de g, on a :

$$\begin{array}{rcl} (g \circ f)(\lambda \cdot x + y) & = & g(f(\lambda \cdot x + y)) \\ & = & g(\lambda \cdot f(x) + f(y)) \\ & = & \lambda \cdot g(f(x)) + g(f(y)) \\ & = & \lambda \cdot (g \circ f)(x) + g \circ f(y) \end{array}$$

Ce qui prouve que $g \circ f \in \mathcal{L}_{\mathbb{K}}(E,G)$.

(ii) Montrons que $g \circ f = 0 \iff \mathrm{Im} f \subset \ker g$.

$$\begin{array}{rcl} g \circ f = 0 & \iff & \forall x \in E\ ,\ g(f(x)) = 0 \\ & \iff & \forall y \in f(E)\ ,\ g(y) = 0 \\ & \iff & \forall y \in \mathrm{Im} f\ ,\ g(y) = 0 \\ & \iff & \forall y \in \mathrm{Im} f\ ,\ y \in \ker g \\ & \iff & \mathrm{Im} f \subset \ker g \end{array}$$

• Montrons 2.

Pour commencer, on vient de prouver que $\mathcal{L}_{\mathbb{K}}(E,F)$, $\mathcal{L}_{\mathbb{K}}(F,G)$ et $\mathcal{L}_{\mathbb{K}}(E,G)$ sont des $\mathbb{K}$-espaces vectoriels. Il y a donc un sens à parler d'application linéaire ou bilinéaire de $\mathcal{L}_{\mathbb{K}}(E,F) \times \mathcal{L}_{\mathbb{K}}(F,G)$ dans $\mathcal{L}_{\mathbb{K}}(E,G)$.

Par ailleurs, d'après la propriété 1, l'application φ est bien définie car tout $(g,f) \in \mathcal{L}_{\mathbb{K}}(F,G) \times \mathcal{L}_{\mathbb{K}}(E,F)$, $\varphi(g,f) = g \circ f \in \mathcal{L}_{\mathbb{K}}(E,G)$. Il reste donc à prouver que φ est bilinéaire.

Montrons que φ est linéaire à droite, c'est-à-dire :

$$\forall g \in \mathcal{L}(F,G)\ ,\ \forall f_1, f_2 \in \mathcal{L}(E,F)\ ,\ \forall \lambda \in \mathbb{K}\ ,\ g\circ(\lambda\cdot f_1+f_2) = \lambda\cdot(g\circ f_1)+g\circ f_2$$

Soient $g \in \mathcal{L}(F,G)$, $f_1, f_2 \in \mathcal{L}(E,F)$, $\lambda \in \mathbb{K}$. Alors,

$$\begin{array}{rcl} \forall x \in E\ ,\ \varphi(g, \lambda\cdot f_1 + f_2)(x) & = & \Big(g \circ (\lambda\cdot f_1 + f_2)\Big)(x) \\ & = & g\big((\lambda\cdot f_1 + f_2)(x)\big) \\ & = & g\big(\lambda\cdot f_1(x) + f_2(x)\big) \end{array}$$

où la dernière égalité est vraie par définition de $+$ et $\cdot$. Ainsi, puisque g est linéaire, on a :

$$\begin{array}{rcl} \forall x \in E\ ,\ \varphi(g, \lambda\cdot f_1 + f_2)(x) & = & \lambda\cdot g(f_1(x)) + g(f_2(x)) \\ & = & (\lambda\cdot(g\circ f_1) + g\circ f_2)(x) \\ & = & \Big(\lambda\cdot\varphi(g,f_1) + \varphi(g,f_2)\Big)(x) \end{array}$$

Ainsi, pour tout $x \in E$, $\varphi(g, \lambda\cdot f_1 + f_2)(x) = (\lambda\cdot\varphi(g,f_1) + \varphi(g,f_2))(x)$, c'est-à-dire $\varphi(g, \lambda\cdot f_1 + f_2) = \lambda\cdot\varphi(g,f_1) + \varphi(g,f_2)$. D'où φ est linéaire à droite.

Montrons que φ est linéaire à gauche, c'est-à-dire :

$$\forall f \in \mathcal{L}(E,F)\ ,\ \forall g_1, g_2 \in \mathcal{L}(F,G)\ ,\ \forall \lambda \in \mathbb{K}\ ,\ (\lambda\cdot g_1+g_2)\circ f = \lambda\cdot(g_1\circ f)+g_2\circ f$$

La linéarité à gauche est évidente et toujours vraie dans le sens où on n'utilise pas du tout le fait que g_1, g_2 ou f sont linéaires. ⊠

⚠ **Attention :** $(\mathcal{F}(E,E), +, \circ)$ n'est pas un anneau en général. La démonstration précédente montre que $\circ$ est distributive à gauche par rapport à $+$ mais pas à droite !

Exemple 4.4.4.4 Soient $E = \mathbb{R}$, $\forall x \in \mathbb{R}$, $f(x) = x$, et $\forall x \in \mathbb{R}$, $g(x) = x^2$. Alors :

$$\forall x \in \mathbb{R}\ ,\ \Big(g \circ (f+f)\Big)(x) = g(f(x)+f(x)) = g(2x) = 4x^2$$

mais

$$\forall x \in \mathbb{R}\ ,\ \Big(g\circ f + g\circ f\Big)(x) = g(f(x)) + g(f(x)) = 2x^2$$

Théorème 4.4.4.5 *Soit E un $\mathbb{K}$-espace vectoriel. Alors :*

(i) $(\mathcal{L}(E), +, \circ)$ *est un anneau (non commutatif si* $E \neq \{0\}$ *et n'est pas une droite vectorielle) ;*

(ii) $(\mathcal{L}(E), +, \cdot)$ *est un* $\mathbb{K}$*-espace vectoriel ;*

(iii) $\forall (f, g) \in \mathcal{L}(E) \times \mathcal{L}(E)$, $\forall \lambda \in \mathbb{K}$, $\lambda \cdot (g \circ f) = (\lambda \cdot g) \circ f = g \circ (\lambda \cdot f)$.

On dit que $(\mathcal{L}(E), +, \circ, \cdot)$ *est une* $\mathbb{K}$*-algèbre.*

Preuve :

• D'après la proposition 4.4.4.1 avec $F = E$, $(\mathcal{L}_{\mathbb{K}}(E, E), +, \cdot)$, c'est-à-dire $(\mathcal{L}(E), +, \cdot)$ est un $\mathbb{K}$-espace vectoriel.

• Montrons que $(\mathcal{L}(E), +, \circ)$ est un anneau.

∗ $(\mathcal{L}(E), +)$ est un groupe abélien (puisque $(\mathcal{L}(E), +, \cdot)$ est un espace vectoriel) ;

∗ $\circ$ est bien une loi de composition interne d'après le théorème 4.4.4.3 (c'est-à-dire que la composée de deux applications linéaires est encore linéaire) ;

∗ $\circ$ est distributive (à gauche et à droite) par rapport à $+$ (toujours d'après le théorème 4.4.4.3) ;

∗ $\circ$ est associative sur $\mathcal{L}(E)$ puisqu'elle l'est sur $\mathcal{F}(E, E)$ (propriété de la composition d'applications) ;

∗ enfin, Id_E est clairement une application linéaire de E dans E et est neutre pour la loi $\circ$.

Ceci prouve que $(\mathcal{L}(E), +, \circ)$ est un anneau.

• Enfin, la propriété (*iii*) est une conséquence du théorème 4.4.4.3 (la « bilinéarité »).

⊠

Remarque : *si $E \neq \{0\}$ et n'est pas une droite vectorielle, on choisit $x, y \in E$ non colinéaires, on note $F =< x, y >$ et on fixe G un supplémentaire de F dans E. Si f est l'unique application linéaire*[3] *telle que $f(x) = f(y) = y$ et $f_{|G} = 0$ et g celle qui vérifie $g(x) = g(y) = x$ et $g_{|G} = 0$, alors $g \circ f \neq f \circ g$.*

Exercice 4.4.4.6 Montrer que si $E = \mathbb{K}u$ avec $u \in E \setminus \{0_E\}$, alors $\mathcal{L}_{\mathbb{K}}(E) = \mathbb{K}\mathrm{Id}_E$.

3. voir paragraphe suivant sur le recollement des applications linéaires.

4.4.5 Isomorphismes, automorphismes et groupe linéaire

Définition 4.4.5.1 Soient E et F deux $\mathbb{K}$-espaces vectoriels et $f \in F^E$. On dit que :

- f est un isomorphisme d'espaces vectoriels si $f \in \mathcal{L}(E,F)$ et f est bijective ;
- f est un automorphisme de E si f est un isomorphisme de E dans E.

Exemple 4.4.5.2 Si E est un espace vectoriel, alors Id_E est un automorphisme de E.

Exemple 4.4.5.3 L'application f définie par : $\forall (x,y) \in \mathbb{R}^2$, $f(x,y) = (x+y, x-y)$ est un automorphisme de $\mathbb{R}^2$. En effet, on peut vérifier sans difficultés que f est linéaire et bijective (sa bijection réciproque étant donnée par $(a,b) \longmapsto (\frac{a+b}{2}, \frac{a-b}{2})$).

Exemple 4.4.5.4 Soit $(a,b,c) \in \mathbb{C}^3$ (avec $a \neq 0$) et soit $\mathcal{S}_H$ l'ensemble des solutions de l'équation différentielle $(E) : ay'' + by' + cy = 0$. Alors l'application :

$$\varphi : \begin{array}{ccc} \mathcal{S}_H & \longrightarrow & \mathbb{C}^2 \\ y & \longmapsto & (y(0), y'(0)) \end{array}$$

est un isomorphisme d'espaces vectoriels. En effet,

- φ est linéaire car si $(y_1, y_2) \in \mathcal{S}_H^2$ et $(\lambda, \mu) \in \mathbb{C}^2$:

$$\begin{aligned} \varphi(\lambda \cdot y_1 + \mu \cdot y_2) &= \big((\lambda \cdot y_1 + \mu \cdot y_2)(0), (\lambda \cdot y_1 + \mu \cdot y_2)'(0)\big) \\ &= (\lambda y_1(0) + \mu y_2(0), \lambda y_1'(0) + \mu y_2'(0)) \\ &= \lambda \cdot (y_1(0), y_1'(0)) + \mu \cdot (y_2(0), y_2'(0)) \\ &= \lambda \cdot \varphi(y_1) + \mu \cdot \varphi(y_2) \end{aligned}$$

- φ est bijective car d'après le cours sur les équations différentielles, pour tout $(\alpha, \beta) \in \mathbb{C}^2$, il existe une unique solution de (E) vérifiant $y(0) = \alpha$ et $y'(0) = \beta$.

Exemple 4.4.5.5 En revanche, les applications linéaires suivantes ne sont pas des isomorphismes :

- l'application $D : \mathcal{C}^1(\mathbb{R},\mathbb{R}) \longrightarrow \mathcal{C}^0(\mathbb{R},\mathbb{R})$ qui à f associe $D(f) = f'$ (elle est surjective mais non injective) ;
- l'application de $\mathbb{R}$ dans $\mathbb{R}^2$ qui à x associe (x,x) (elle est injective mais non surjective).

Proposition 4.4.5.6 *Soient E, F deux espaces vectoriels et soit f est un isomorphisme (d'espaces vectoriels) de E dans F. Alors $f^{-1} \in \mathcal{L}(F, E)$ et f^{-1} est bijective, c'est-à-dire f^{-1} est un isomorphisme de F dans E.*

Preuve :

• Puisque f est aussi un isomorphisme de groupes de $(E, +)$ dans $(F, +)$, on sait déjà que f^{-1} est un isomorphisme de groupes de $(F, +)$ dans $(E, +)$, c'est-à-dire :

- f^{-1} est une bijection de F dans E ;
- $\forall (y_1, y_2) \in F^2$, $f^{-1}(y_1 + y_2) = f^{-1}(y_1) + f^{-1}(y_2)$.

• Il reste donc à prouver que : $\forall y \in F$, $\forall \lambda \in \mathbb{K}$, $f^{-1}(\lambda \cdot y) = \lambda \cdot f^{-1}(y)$. Soit $(\lambda, y) \in \mathbb{K} \times F$. Puisque f est linéaire,

$$f\left(\lambda \cdot f^{-1}(y)\right) = \lambda \cdot f(f^{-1}(y)) = \lambda \cdot y$$

En prenant l'image par f^{-1}, on obtient le résultat. ⊠

Corollaire 4.4.5.7 *L'ensemble des éléments inversibles de l'anneau $\mathcal{L}(E)$ est un groupe pour la loi $\circ$. Ce groupe est appelé le groupe linéaire de E et est noté $\mathcal{GL}(E)$.*

Preuve :

On montre que $\mathcal{GL}(E)$ un sous-groupe de $(\sigma(E), \circ)$ (groupe de référence constitué des bijections de E dans E).

- pour commencer, $\mathcal{GL}(E) \subset \sigma(E)$ et $\mathrm{Id}_E \in \mathcal{GL}(E)$;
- si $f, g \in \mathcal{GL}(E)$, alors $f \circ g \in \mathcal{L}(E)$ et par suite $f \circ g \in \mathcal{GL}(E)$ (car la composée de deux bijections est une bijection) ;
- enfin, d'après la proposition précédente, si $f \in \mathcal{GL}(E)$, alors f^{-1} (la bijection réciproque de f) est également bijective et linéaire. Par suite, $f^{-1} \in \mathcal{GL}(E)$.

Ce qui prouve que $(\mathcal{GL}(E), \circ)$ est un sous-groupe de $(\sigma(E), \circ)$: c'est donc un groupe. ⊠

Exercice 4.4.5.8 Retrouver directement ce résultat à l'aide de l'exercice 1.2.3.7.

⚠ **Attention :** $\mathcal{GL}(E)$ n'est pas un sev de $\mathcal{L}(E)$ et n'est pas stable par addition !

4.4.6 Restriction et recollement

Les deux propositions suivantes sont évidentes.

Proposition 4.4.6.1 *Soient E, F deux $\mathbb{K}$-espaces vectoriels, A un sous-espace vectoriel de E, et $f \in \mathcal{L}(E,F)$. Alors $f_{|A} \in \mathcal{L}(A,F)$ et de plus,* $\ker(f_{|A}) = \ker(f) \cap A$.

Proposition 4.4.6.2 *Soient E, F deux $\mathbb{K}$-espaces vectoriels et $f \in \mathcal{L}(E,F)$. Alors l'application $\tilde{f} : E \longrightarrow \mathrm{Im}(f)$ qui à x associe $f(x)$ est linéaire.*

Théorème 4.4.6.3 *Soient E, F deux $\mathbb{K}$-espaces vectoriels et $f \in \mathcal{L}(E,F)$. On suppose que* $\ker(f)$ *admet un supplémentaire dans E et on fixe G un supplémentaire de* $\ker(f)$ *dans E. Alors l'application :*

$$\overline{f} : \begin{array}{ccc} G & \longrightarrow & \mathrm{Im}(f) \\ x & \longmapsto & f(x) \end{array}$$

est un isomorphisme d'espaces vectoriels.

Preuve :

- D'après la proposition 4.4.6.2, $\tilde{f} \in \mathcal{L}(E, \mathrm{Im}(f))$.
- D'après la proposition 4.4.6.1, $\overline{f} = \tilde{f}_{|G} \in \mathcal{L}(G, \mathrm{Im}(f))$ et :

$$\ker(\overline{f}) = \ker(\tilde{f}) \cap G = \ker(f) \cap G = \{0\}$$

(puisque $G \oplus \ker(f)$). Par suite, $\overline{f}$ est injective.

- Montrons enfin que $\overline{f}$ est surjective.
Soit $y \in \mathrm{Im}(f)$. Par définition, il existe $x \in E$ tel que $y = f(x)$. Or, $\ker(f) \oplus G = E$ donc il existe (un unique) $(a,b) \in \ker(f) \times G$ tel que $x = a + b$. On a alors :

$$y = f(a) = f(a+b) = f(a) + f(b) = f(b) = \overline{f}(b)$$

(car d'une part $f(a) = 0$ puisque $a \in \ker(f)$ et $\overline{f}(b) = f(b)$ car $b \in G$).
Ce qui prouve que $\overline{f}$ est surjective.

⊠

Théorème 4.4.6.4 *Soient E et F deux $\mathbb{K}$-espaces vectoriels, G et H deux sous-espaces vectoriels supplémentaires dans E. Alors l'application :*

$$\begin{array}{rcl} \varphi : \mathcal{L}(E,F) & \longmapsto & \mathcal{L}(G,F) \times \mathcal{L}(H,F) \\ f & \longmapsto & (f_{|G}, f_{|H}) \end{array}$$

est un isomorphisme de $\mathbb{K}$-espaces vectoriels. En clair, la connaissance d'une application linéaire sur deux sous-espaces vectoriels supplémentaires détermine l'application linéaire de façon unique.

Preuve :

• Tout d'abord, d'après ce qui précède, $\mathcal{L}(E,F)$, $\mathcal{L}(G,F)$ et $\mathcal{L}(H,F)$ sont des $\mathbb{K}$-espaces vectoriels. Par suite, $\mathcal{L}(G,F) \times \mathcal{L}(H,F)$ est aussi un $\mathbb{K}$-espace vectoriel.

• Ensuite, d'après la proposition 4.4.6.1, pour tout $f \in \mathcal{L}(E,F)$, on a $f_{|G} \in \mathcal{L}(G,F)$ et $f_{|H} \in \mathcal{L}(H,F)$. Par conséquent, φ est bien définie.

• Par ailleurs, pour toutes $f, g \in \mathcal{L}(E,F)$, pour tous $\lambda, \mu \in \mathbb{K}$, et pour tout sous-espace vectoriel A de E, $(\lambda \cdot f + \mu \cdot g)_{|A} = \lambda \cdot (f_{|A}) + \mu \cdot (g_{|A})$. Par suite, φ est linéaire.

• Montrons enfin que φ est bijective.

∗ Injectivité

Soit $f \in \ker(\varphi)$. Montrons que $f = 0$. Par définition de φ, $f_{|G} = 0$ et $f_{|H} = 0$. Soit alors $x \in E$. Puisque G et H sont supplémentaires dans E, il existe un unique couple $(a,b) \in G \times H$ tel que $x = a + b$. On a alors :

$$\begin{array}{rcll} f(x) & = & f(a+b) & \\ & = & f(a) + f(b) & \text{(puisque } f \in \mathcal{L}(E,F)\text{)} \\ & = & f_{|G}(a) + f_{|H}(b) & \text{(puisque } a \in G \text{ et } b \in H\text{)} \\ & = & 0 + 0 & \text{(puisque } f_{|G} = 0 \text{ et } f_{|H} = 0\text{)} \\ & = & 0 & \end{array}$$

Par conséquent, pour tout $x \in E$, $f(x) = 0$, c'est-à-dire $f = 0$ (application nulle) et $\ker(\varphi) = \{0\}$, c'est-à-dire φ est injective.

∗ Surjectivité

Soient $g \in \mathcal{L}(G,F)$ et $h \in \mathcal{L}(H,F)$. Montrons qu'il existe une application $f \in \mathcal{L}(E,F)$ telle que $f_{|G} = g$ et $f_{|H} = h$.
Soit $x \in E$: il existe un unique couple $(a,b) \in G \times H$ tel que $x = a + b$. On pose alors $f(x) = g(a) + h(b)$.

Ceci définit bien une application f de E dans F puisque pour chaque $x \in E$, le couple $(a, b) \in G \times H$ est unique. Montrons alors que f convient.

- ▷ Si $x \in G$, alors par unicité du couple $(a, b) \in G \times H$ tel que $x = a + b$, on a $a = x$ et $b = 0$. Alors,

$$f(x) = g(a) + h(b) = g(x) + h(0) = g(x) + 0 = g(x)$$

  Par suite, $f_{|G} = g$.

- ▷ De la même façon, on montre que $f_{|H} = h$.

- ▷ Montrons enfin que $f \in \mathcal{L}(E, F)$.
  Soient $x, x' \in E$ et $\lambda \in \mathbb{K}$. Il existe alors un unique couple $(a, b) \in G \times H$ et un unique couple $(a', b') \in G \times H$ tels que $x = a + b$ et $x' = a' + b'$. On a alors :

$$\lambda \cdot x + x' = (\lambda \cdot a + a') + (\lambda \cdot b + b')$$

  Puisque G et H sont des sous-espaces vectoriels de E, on en déduit que $(\lambda \cdot a + a', \lambda \cdot b + b') \in G \times H$. Par suite,

$$\begin{array}{rcl} f(\lambda \cdot x + x') & = & g(\lambda \cdot a + a') + h(\lambda \cdot b + b') \\ & = & \lambda \cdot g(a) + g(a') + \lambda \cdot h(b) + h(b') \\ & = & \lambda \cdot (g(a) + h(b)) + g(a') + h(b') \\ & = & \lambda \cdot f(x) + f(x') \end{array}$$

  Ce qui prouve que f est une application linéaire.

Ainsi, on a montré que pour tout $(g, h) \in \mathcal{L}(G, F) \times \mathcal{L}(H, F)$ il existe $f \in \mathcal{L}(E, F)$ telle que $f_{|G} = g$ et $f_{|H} = h$, c'est-à-dire $\varphi(f) = (g, h)$. Par conséquent, φ est surjective.

⊠

Exemple 4.4.6.5 Dans le plan $\overrightarrow{\mathcal{P}}$ qu'on munit de la base orthonormée directe usuelle $(\vec{i}, \vec{j})$, on considère $G =< \vec{i} >= \mathbb{R}\vec{i}$ et $H =< \vec{j} >= \mathbb{R}\vec{j}$. Alors G et H sont des sous-espaces vectoriels supplémentaires de $\overrightarrow{\mathcal{P}}$. Il existe donc un unique endomorphisme p de $\overrightarrow{\mathcal{P}}$ tel que : $p_{|G} = i_{G,\overrightarrow{\mathcal{P}}}$ (application inclusion) et $p_{|H} = 0$. À quoi correspond l'application p ?

Remarques :

- *ceci justifie l'existence (et l'unicité) des applications f et g données dans la remarque (après le théorème 4.4.4.5) permettant de prouver que si E contient au moins deux vecteurs non colinéaires, alors $\mathcal{L}(E)$ est un anneau non commutatif) ;*
- *ce théorème nous permettra de définir de façon « simple » les notions de projecteur et de symétrie (voir le paragraphe sur les applications linéaires remarquables).*

4.4.7 Hyperplans d'un espace vectoriel et formes linéaires

Définition 4.4.7.1 Soit E un $\mathbb{K}$-espace vectoriel. On appelle hyperplan de E tout sous-espace vectoriel H de E qui admet pour supplémentaire une droite vectorielle. Autrement dit, un sous-espace vectoriel H de E est un hyperplan de E si :

$$\exists u \in E \setminus \{0_E\} \ , \ H \oplus \mathbb{K}u = E$$

Exemple 4.4.7.2 Dans le plan usuel $\overrightarrow{\mathcal{P}}$, un hyperplan est une droite vectorielle.

Exemple 4.4.7.3 Dans l'espace $\overrightarrow{\mathcal{E}}$, un hyperplan est un plan vectoriel.

Exemple 4.4.7.4 Dans $\mathbb{R}^4$, l'ensemble $H = \{(x, y, z, t) \in \mathbb{R}^4 \ / \ t = 0\}$ est un hyperplan. En effet, on peut vérifier (le faire) que $H \oplus \mathbb{R}(0, 0, 0, 1) = \mathbb{R}^4$. Remarquez qu'on peut aussi choisir une autre droite vectorielle. On a aussi $H \oplus \mathbb{R}(1, 0, 0, 1) = \mathbb{R}^4$.

Exercice 4.4.7.5 Montrer que $H = \{(u_n)_{n\in\mathbb{N}} \in \mathbb{R}^{\mathbb{N}} \mid u_0 = 0\}$ est un hyperplan de $\mathbb{R}^{\mathbb{N}}$.

Proposition 4.4.7.6 *Soient E un $\mathbb{K}$-espace vectoriel, H un hyperplan de E et $x \in E$. Alors :*

$$H \oplus \mathbb{K}x = E \iff x \notin H$$

Preuve :

Il est évident que si $H \oplus \mathbb{K}x = E$, alors $x \notin H$. Réciproquement, si $x \notin H$, il est évident que $H \oplus \mathbb{K}x$ (c'est-à-dire que ces deux espaces vectoriels sont en somme directe). Montrons que la somme vaut E.
Par définition d'un hyperplan, il existe $u \in E \setminus \{0\}$ tel que $H \oplus \mathbb{K}u = E$ et puisque $x \in E$, il existe $h \in H$ et $\lambda \in \mathbb{K}$ (qui sont uniques) tels que $x = h + \lambda u$. Or, $x \notin H$ donc $\lambda \neq 0$ et on a donc :

$$u = \frac{1}{\lambda} \cdot x - \frac{1}{\lambda} h \in \mathbb{K}x + H$$

On en déduit donc que $\mathbb{K}u \subset (\mathbb{K}x + H)$ et de même, $H \subset (\mathbb{K}x + H)$. Par suite,

$$E = H + \mathbb{K}u \subset H + \mathbb{K}x \subset E$$

⊠

Théorème 4.4.7.7 *Soit E un $\mathbb{K}$-espace vectoriel et soit $H \subset E$. Alors les énoncés suivants sont équivalents :*

(i) H est un hyperplan de E ;

(ii) il existe f une forme linéaire sur E, non nulle, telle que : $H = \ker(f)$.

Par ailleurs, si $f, g \in \mathcal{L}_{\mathbb{K}}(E, \mathbb{K}) \setminus \{0\}$ (c'est-à-dire f et g sont deux formes linéaires non nulles sur E), alors :

$$\ker(f) = \ker(g) \iff \exists \lambda \in \mathbb{K}^\star \ , \ g = \lambda f$$

Preuve :

• Montrons $(i) \Longrightarrow (ii)$

On suppose que H est un hyperplan de E. Alors il existe $u \in E \setminus \{0\}$ tel que $H \oplus < u >= E$. D'après le théorème de recollement, il existe une unique application linéaire $f \in \mathcal{L}(E, \mathbb{K})$ telle que :

$$\forall x \in H \ , \ f(x) = 0_{\mathbb{K}} \quad \text{et} \quad \forall \lambda \in \mathbb{K} \ , \ f(\lambda \cdot u) = \lambda$$

Il est alors clair que $H = \ker(f)$ et que f est une forme linéaire non nulle (puisque $f(u) = 1_{\mathbb{K}}$ par exemple).

• Réciproquement, supposons que $H = \ker(f)$ avec f une forme linéaire non nulle sur E. Montrons que H est un hyperplan.
Par hypothèse, f n'est pas identiquement nulle. Il existe donc $u \in E$ tel que $f(u) \neq 0_{\mathbb{K}}$. f étant linéaire, on a donc nécessairement $u \neq 0_E$.

Montrons que $E = \ker(f) \oplus \mathbb{K}u$.

* Montrons que $\ker(f) \cap \mathbb{K}u = \{0_E\}$.
Soit $x \in \ker(f) \cap \mathbb{K}u$. D'une part, $x \in \mathbb{K}u$ donc il existe $\lambda \in \mathbb{K}$ tel que $x = \lambda \cdot u$. Par ailleurs, $x \in \ker(f)$ donc $0_{\mathbb{K}} = f(x)$. Il s'ensuit que :
$$0 = f(x) = f(\lambda u) = \lambda \cdot f(u) = \lambda \times f(u)$$
Or, $f(u) \neq 0_{\mathbb{K}}$ donc $\lambda = 0_{\mathbb{K}}$ (car $\mathbb{K}$ est un corps *a fortiori* un anneau intègre) et $x = 0_{\mathbb{K}} \cdot u = 0_E$.

* Montrons que $E = \ker(f) + < u >$.
Soit $x \in E$. Sachant que $f(u) \neq 0_{\mathbb{K}}$, $f(u)$ est inversible dans $\mathbb{K}$. On peut alors écrire :
$$x = \big(x - f(x)f(u)^{-1}u\big) + f(x)f(u)^{-1}u$$

On a par définition, $f(x)f(u)^{-1}u \in \mathbb{K}u$. Par conséquent, on pose $h = x - f(x)f(u)^{-1}u$ et on a :

$$f(h) = f(x) - f(x)f(u)^{-1}f(u) = f(x) - f(x) = 0_{\mathbb{K}}$$

c'est-à-dire $h \in \ker(f)$. On a donc montré qu'il existe $h \in \ker(f)$ et $\lambda \in \mathbb{K}$ tels que : $x = h + \lambda u$. Ceci prouve que $E = \ker(f) + \mathbb{K}u$.

• Enfin, montrons que si f et g sont deux formes linéaires non nulles, alors $\ker(f) = \ker(g)$ si et seulement si il existe $\lambda \in \mathbb{K}^\star$ tel que $g = \lambda f$.

∗ L'implication $\Longleftarrow$ est évidente. En effet, si $g = \lambda f$ avec $\lambda \neq 0$, alors $f(x) = 0 \iff g(x) = 0$.

∗ Montrons $\Longrightarrow$.
On suppose que $\ker(f) = \ker(g) = H$. D'après ce qui précède, H est un hyperplan de E : il existe donc $u \in E \setminus \{0_E\}$ tel que $H \oplus \mathbb{K}u = E$. On a alors $f(u) \neq 0_{\mathbb{K}}$ et $g(u) \neq 0_{\mathbb{K}}$. On pose $\lambda = g(u)f(u)^{-1}$. Montrons que $g = \lambda \cdot f$.
Si $x \in H$, alors $g(x) = 0_{\mathbb{K}} = f(x) = \lambda \cdot f(x)$.
Si $\alpha \in \mathbb{K}$, alors :

$$g(\alpha \cdot u) = \alpha \cdot g(u) = \alpha \times g(u) = g(u) \times f(u)^{-1} \times \alpha \times f(u) = \lambda \cdot f(\alpha \cdot u)$$

Ainsi, $g_{|H} = \lambda \cdot f_{|H}$ et $g_{|<u>} = \lambda \cdot f_{|<u>}$. D'après le théorème de recollement, $g = \lambda \cdot f$. ⊠

Remarques :

- *il ne faut pas oublier l'hypothèse de non nullité de la forme linéaire considérée ;*
- *dans la démonstration, pour montrer que $H = \ker(f)$ est un hyperplan, on sait qu'on doit choisir $u \in E \setminus \ker(f)$ et la proposition précédente nous dit que si H est un hyperplan, on doit avoir $E = \ker(f) \oplus \mathbb{K}u$. Ensuite, pour trouver la décomposition, on pouvait aussi procéder par analyse-synthèse pour trouver la décomposition $x = (x - \frac{f(x)}{f(u)}u) + \frac{f(x)}{f(u)}u$;*
- *de la même façon, lorsque l'on prouve que f et g sont proportionnelles, on peut trouver le coefficient en raisonnant par analyse-synthèse ;*
- *moralement, ce théorème est assez simple à comprendre. Dans $\mathbb{R}^3$, un hyperplan est simplement un plan vectoriel et on sait qu'un plan a pour équation cartésienne $ax + by + cz = 0$ (avec $(a, b, c) \neq (0, 0, 0)$), ce qui correspond au noyau de la forme linéaire $(x, y, z) \longmapsto ax + by + cz$. Dans un cadre un peu plus général, c'est le « f » qui donne « une équation de l'hyperplan ». De plus, toujours dans $\mathbb{R}^3$, il est évident que deux plans sont égaux si et seulement si leurs équations cartésiennes sont proportionnelles. La généralisation est donc que f et g sont proportionnelles ;*
- *on reverra d'autres explications simples lors du chapitre sur la dimension d'un espace vectoriel (cours de mathématiques supérieures 2).*

4.4.8 Étude d'applications linéaires remarquables

Dans ce paragraphe, E est un $\mathbb{K}$-espace vectoriel sur un corps commutatif $\mathbb{K}$.

4.4.8.a Homothéties

Définition 4.4.8.1 On dit qu'une application $h \in \mathcal{F}(E,E)$ est une homothétie s'il existe $\lambda \in \mathbb{K}$ tel que $h = \lambda \cdot \mathrm{Id}_E$.

Proposition 4.4.8.2 *L'ensemble $\mathcal{H}(E)$ des homothéties de E est une sous-algèbre commutative de $\mathcal{L}(E)$, c'est-à-dire un sous-espace vectoriel et un sous-anneau commutatif de $\mathcal{L}(E)$.*
Par ailleurs, l'ensemble des homothéties non nulles est un sous-groupe commutatif de $\mathcal{GL}(E)$, isomorphe à $(\mathbb{K}^\star, \times)$.

Preuve :

Pour $\lambda \in \mathbb{K}$, on note $h_\lambda = \lambda \cdot \mathrm{Id}_E$. On montre de façon évidente que pour tout $(\lambda,\mu) \in \mathbb{K}^2$, on a les relations :

$$h_\lambda + h_\mu = h_{\lambda+\mu} \ , \ h_\lambda \circ h_\mu = h_\mu \circ h_\lambda = h_{\lambda\times\mu} \quad \text{et } \lambda \cdot h_\mu = h_{\lambda\times\mu}$$

On en déduit alors que $\mathcal{H}(E)$ est une sous-algèbre commutative de $\mathcal{L}(E)$. Je vous laisse faire la démonstration précise en exercice.

Par ailleurs, on a aussi : $h_{1_\mathbb{K}} = \mathrm{Id}_E \quad$ et $\quad \forall \lambda \in \mathbb{K}^\star \ , \ h_\lambda^{-1} = h_{\lambda^{-1}}$.
Par suite, $\mathcal{H}'(E) = \mathcal{H}(E) \setminus \{0\} = \mathbb{K}^\star \mathrm{Id}_E$ est un sous-groupe commutatif de $\mathcal{GL}(E)$ et l'application :

$$\begin{array}{rccc} \varphi : & (\mathbb{K}^\star, \times) & \longrightarrow & (\mathcal{H}'(E), \circ) \\ & \lambda & \longmapsto & h_\lambda \end{array}$$

est un isomorphisme de groupes.

⊠

Remarque : *c'est un cas très particulier ! Comme vous l'avez déjà vu dans ce chapitre, l'ensemble $\mathcal{L}(E)$ n'est pas commutatif en général.*

Exercice 4.4.8.3 Comment interpréter géométriquement le signe de λ ? Et la position de $|\lambda|$ par rapport à 1 ?

4.4.8.b Projecteurs

Définition 4.4.8.4 Soient E un $\mathbb{K}$-espace vectoriel, F et G deux sous-espaces vectoriels supplémentaires dans E. On appelle projection sur F parallèlement à G l'unique application linéaire de E dans E vérifiant :

$$p_{|F} = \mathrm{Id}_F \quad \text{et} \quad p_{|G} = 0$$

Le projecteur sur F parallèlement à G est noté $p_{F//G}$.

Remarques :

- *cette définition a un sens d'après le théorème de recollement des applications linéaires. Autrement dit, il existe bien un et un seul endomorphisme de E vérifiant $p_{|F} = Id_F$ et $p_{|G} = 0$;*
- *dans la définition précédente, on commet un abus de notation car p est à valeurs dans E. En toute rigueur, il faudrait écrire que $p_{|F}$ est égal à l'inclusion de F dans E ;*
- *on retient aussi que si $x \in E$, alors x s'écrit de façon unique $x = x_F + x_G$ avec $x_F \in F$ et $x_G \in G$ et que dans ce cas, par définition, $p_{F//G}(x) = x_F$.*

Exemple 4.4.8.5 Dans $\mathbb{R}^3$, on considère le plan $F = \{(x, y, z) \in \mathbb{R}^3 \ / \ z = 0\}$ et la droite $G = F^\perp = \mathbb{R} < 0, 0, 1 >$. Alors la projection sur F parallèlement à G est la projection orthogonale « usuelle » sur le plan F.

Exemple 4.4.8.6 L'application $p : \mathcal{F}(\mathbb{R}, \mathbb{R}) \longrightarrow \mathcal{F}(\mathbb{R}, \mathbb{R})$ qui à une application f associe $p(f) : x \longmapsto \frac{f(x)+f(-x)}{2}$ est la projection sur $\mathcal{P}$ (ensemble des applications paires) parallèlement à $\mathcal{I}$ (l'ensemble des applications impaires). En effet,

$$\mathcal{P} \oplus \mathcal{I} = \mathcal{F}(\mathbb{R}, \mathbb{R}) \text{ et } p_{|\mathcal{P}} = \mathrm{Id}_{\mathcal{P}} \text{ et } p_{|\mathcal{I}} = 0$$

Définition 4.4.8.7 Soit E un $\mathbb{K}$-espace vectoriel. On appelle projecteur de E tout endomorphisme de E tel qu'il existe F et G, deux sous-espaces vectoriels supplémentaires dans E tels que $p = p_{F//G}$.

À partir de cette définition, il n'est pas toujours « évident » de reconnaître un projecteur car cela suppose qu'on « connaît F et G ». Les propriétés qui suivent vont donner une description explicite des ensembles « F et G » et fournir un critère simple pour reconnaître un projecteur et ses éléments caractéristiques, c'est-à-dire « F et G ».

Proposition 4.4.8.8 *Soient E un $\mathbb{K}$-espace vectoriel, F et G deux sous-espaces vectoriels supplémentaires dans E et $p = p_{F//G}$ le projecteur sur F parallèlement à G. Alors :*

(i) $\ker(p) = G$ *et* $\mathrm{Im}(p) = F$ *;*

(ii) $\forall x \in E\ ,\ (x \in \mathrm{Im}(p) \iff p(x) = x)$, *autrement dit* $\mathrm{Im}(p) = \ker(Id_E - p)$.

Preuve :

• Montrons que $\ker(p) = G$.
Soit $x \in E$. Puisque F et G sont supplémentaires dans E, il existe un unique couple $(x_F, x_G) \in F \times G$ tel que $x = x_F + x_G$. On a alors :

$$\begin{aligned} x \in \ker(p) &\iff p(x_F + x_G) = 0 \\ &\iff p(x_F) + p(x_G) = 0 \\ &\iff x_F = 0 \\ &\iff x \in G \end{aligned}$$

Par suite, $\ker(p) = G$.

• Montrons que $\mathrm{Im}(p) = F$ par double inclusion.

∗ $\mathrm{Im}(p) \subset F$
Soit $y \in \mathrm{Im}(p)$. Il existe $x \in E$ tel que $y = p(x)$. Par ailleurs, il existe $(x_F, x_G) \in F \times G$ tel que $x = x_F + x_G$. On a alors : $y = p(x) = x_F \in F$.

∗ $F \subset \mathrm{Im}(p)$
Soit $x_F \in F$. Alors $p(x_F) = x_F$ donc $x_F \in \mathrm{Im}p$.

• Enfin, soit $x \in E$.

∗ Si $x \in \mathrm{Im}(p)$, alors puisque $F = \mathrm{Im}(p)$ et $p = p_{F//G}$, $p(x) = x$ (en fait on l'a déjà prouvé juste au-dessus quand on a montré que $\mathrm{Im}(p) = F$).

∗ Réciproquement, si $x = p(x)$, alors par définition $p(x) \in \mathrm{Im}(p)$ donc $x = p(x) \in \mathrm{Im}(p)$.

⊠

On en déduit immédiatement le corollaire suivant :

Corollaire 4.4.8.9 *Si p est un projecteur de E, alors* $\mathrm{Im}(p) \oplus \ker(p) = E$.

⚠ **Attention :** la réciproque est très fausse ! Par exemple, dans $\mathbb{R}^2$, si $p((x,y)) = (2x, 0)$, alors p est linéaire, $\ker(p) = \mathbb{R}(0,1)$ et $\mathrm{Im}(p) = \mathbb{R}(1,0)$. On a donc bien $\mathrm{Im}(p) \oplus \ker(p) = \mathbb{R}^2$ et pourtant p n'est pas un projecteur puisque $p_{|\mathrm{Im}(p)} = 2\mathrm{Id}_{\mathrm{Im}(p)} \neq \mathrm{Id}_{\mathrm{Im}(p)}$.

Exercice 4.4.8.10 Si $p \in \mathcal{L}(E)$ vérifie $\mathrm{Im}(p) \oplus \ker(p) = E$, à quelle condition nécessaire et suffisante p est-il un projecteur ?

Théorème 4.4.8.11 (Caractérisation des projecteurs) *Soit $p \in \mathcal{L}(E)$. Alors les énoncés suivants sont équivalents :*

(i) p est un projecteur de E ;

(ii) $p \circ p = p$.

Preuve :

• Montrons $\Longrightarrow$.
Si p est un projecteur de E, alors d'après la proposition précédente, $\mathrm{Im}(p) = \ker(\mathrm{Id}_E - p)$ et *a fortiori*, $\mathrm{Im}(p) \subset \ker(\mathrm{Id}_E - p)$. On en déduit donc (théorème 4.4.4.3) que $(\mathrm{Id}_E - p) \circ p = 0$, c'est-à-dire $p \circ p = p$.

• Montrons $\Longleftarrow$.
On suppose que $p^2 = p$. Montrons que $p = p_{\mathrm{Im}(p)//\ker(p)}$.

∗ Tout d'abord, p étant une application linéaire, $\ker(p)$ et $\mathrm{Im}(p)$ sont des sous-espaces vectoriels de E.

∗ Ensuite, montrons que $\ker(p) \oplus \mathrm{Im}(p) = E$.

▷ Montrons que $\mathrm{Im}(p) + \ker(p) = E$.
Soit $x \in E$. Alors $x = p(x) + (x - p(x))$. Or, $p(x) \in \mathrm{Im}(p)$ et $p(x - p(x)) = p(x) - p(p(x)) = p(x) - p(x) = 0$ donc $(x - p(x)) \in \ker(p)$. Par suite, $x \in \ker(p) + \mathrm{Im}(p)$ et donc, on a bien $\mathrm{Im}(p) + \ker(p) = E$.

▷ Montrons que $\mathrm{Im}\ (p) \cap \ker(p) = \{0\}$
Soit $x \in \ker(p) \cap \mathrm{Im}(p)$. Alors il existe $t \in E$ tel que $x = p(t)$. On a aussi $p(x) = 0$, c'est-à-dire $p^2(t) = 0$. Or, par hypothèse $p^2 = p$ donc $p(t) = 0$, c'est-à-dire $x = 0$.
Ce qui prouve que $\ker(p) \oplus \mathrm{Im}(p) = E$.

∗ Enfin, l'égalité $p_{|\ker(p)} = 0$ est claire et si $y \in \mathrm{Im}(p)$, alors il existe $x \in E$ tel que $y = p(x)$ et dans ce cas, $p(y) = p^2(x) = p(x) = y$. D'où $p_{|\mathrm{Im}(p)} = \mathrm{Id}_{\mathrm{Im}(p)}$.

⊠

Proposition 4.4.8.12 *Soient E un $\mathbb{K}$-espace vectoriel et p un projecteur de E. Alors :*

(i) $q = Id_E - p$ *est un projecteur de* E. q *est appelé le projecteur associé à* p *;*

(ii) $\ker(q) = \mathrm{Im}(p)$ *et* $\mathrm{Im}(q) = \ker(p)$.

Preuve :

• Puisque $p \in \mathcal{L}(E)$, $q \in \mathcal{L}(E)$ et de plus, sachant que $p^2 = p$, on a :

$$q^2 = (\mathrm{Id}_E - p)^2 = \mathrm{Id}_E - 2p + p^2 = \mathrm{Id}_E - p = q$$

Ce qui prouve que q est un projecteur.

• Puisque q est un projecteur, $\mathrm{Im}(q) = \ker(\mathrm{Id}_E - q) = \ker(p)$ et de même, par symétrie des rôles de p et q, $\ker(q) = \mathrm{Im}(p)$.

⊠

Remarques :

- *en clair, la proposition précédente dit que si* $p = p_{F//G}$ *alors le projecteur associé* q *est* $q = p_{G//F}$ *;*
- *ceci nous permet aussi de revenir à la preuve du théorème de recollement. Pour prouver la surjectivité, on a en fait considéré* $f = g \circ p_{G//H} + h \circ p_{H//G}$.

Exercice 4.4.8.13 Proposer une autre démonstration de la proposition précédente en revenant à la définition d'un projecteur.

Exercice 4.4.8.14 Soit p l'application de $\mathbb{R}^2$ dans lui-même définie par :

$$\forall (x, y) \in \mathbb{R}^2 \ , \ p((x, y)) = \left(\frac{2x + 2y}{3}, \frac{x + y}{3} \right)$$

Montrer que p est un projecteur de $\mathbb{R}^2$ et préciser ses éléments caractéristiques.

Exercice 4.4.8.15 Soit $E =< \mathrm{ch}, \mathrm{sh} >$ et p l'application définie par :

$$\forall y \in E \ , \ p(y) = y' + y$$

1. Montrer que p est un endomorphisme de E.
2. Montrer que p est un projecteur et déterminer ses éléments caractéristiques.

4.4.8.c Symétries

Définition 4.4.8.16 Soient E un $\mathbb{K}$-espace vectoriel, F et G deux sous-espaces vectoriels supplémentaires dans E. On appelle symétrie par rapport à F parallèlement à G l'unique application linéaire s vérifiant :

$$s_{|F} = \mathrm{Id}_F \quad \text{et} \quad s_{|G} = -\mathrm{Id}_G$$

La symétrie par rapport à F parallèlement à G est notée $s_{F//G}$.

Remarques :

- *par définition, si $x = x_F + x_G$ avec $(x_F, x_G) \in F \times G$, alors $s(x) = x_F - x_G$;*
- *on commet le même abus de notation que dans la définition d'un projecteur.*

Proposition 4.4.8.17 *Soient s la symétrie sur F parallèlement à G et p le projecteur sur F parallèlement à G. Alors :*

$$\ker(s - Id_E) = F \quad ; \quad \ker(s + Id_E) = G \quad et \quad s = 2p - Id_E$$

En particulier, on a donc $\ker(s - Id_E) \oplus \ker(s + Id_E) = E$.

Preuve :

• Soit $x \in E$. Il existe un unique $(x_F, x_G) \in F \times G$ tel que $x = x_F + x_G$. On a alors :

$$s(x) = x \iff x_F - x_G = x_F + x_G \iff x_G = 0 \iff x \in F$$

Ce qui montre dans un premier temps que $\ker(s - \mathrm{Id}_E) = F$.

• On montre de façon similaire que $\ker(s + \mathrm{Id}_E) = G$.

• Enfin, pour l'égalité $s = 2p - \mathrm{Id}_E$, il suffit de faire la vérification sur F, puis sur G.

⊠

Définition 4.4.8.18 Soit E un $\mathbb{K}$-espace vectoriel. On appelle symétrie de E tout endomorphisme de E tel qu'il existe F et G, deux sous-espaces vectoriels supplémentaires dans E tels que $s = s_{F//G}$.

Théorème 4.4.8.19 *Soit $s \in \mathcal{L}(E)$. Alors s est une symétrie de E si et seulement si $s \circ s = Id_E$.*

Preuve :

• Si $s = s_{F//G}$ est une symétrie, alors $s^2_{|F} = \mathrm{Id}_F$ et $s^2_{|G} = \mathrm{Id}_G$ donc d'après le théorème de recollement, $s^2 = \mathrm{Id}_E$.

• Réciproquement, on suppose que $s^2 = \mathrm{Id}_E$.

∗ Montrons que $\ker(s - \mathrm{Id}_E) \oplus \ker(s + \mathrm{Id}_E) = E$.
Soit $x \in E$. Montrons que x s'écrit de façon unique $x = x_1 + x_2$ avec $x_1 \in \ker(s - \mathrm{Id}_E)$ et $x_2 \in \ker(s + \mathrm{Id}_E)$ par analyse-synthèse.

Analyse
Supposons que de tels x_1, x_2 existent. Alors $s(x) = s(x_1) + s(x_2)$ et donc $s(x) = x_1 - x_2$. Or, $x = x_1 + x_2$. Par suite, (en faisant la somme puis la différence),

$$x_1 = \frac{1}{2}(x + s(x)) \quad \text{et} \quad x_2 = \frac{1}{2}(x - s(x))$$

Ce qui prouve l'unicité sous réserve d'existence.

Synthèse
On pose $x_1 = \frac{1}{2}(x + s(x))$ et $x_2 = \frac{1}{2}(x - s(x))$. Alors :

$$s(x_1) = \frac{1}{2}(s(x) + s^2(x)) = \frac{1}{2}(s(x) + x) = x_1$$

Par suite, $x_1 \in \ker(s - \mathrm{Id}_E)$. On montre de la même façon que $x_2 \in \ker(s + \mathrm{Id}_E)$. Enfin, il est évident que $x = x_1 + x_2$.

Ce qui prouve que $\ker(s - \mathrm{Id}_E) \oplus \ker(s + \mathrm{Id}_E) = E$.

∗ Par définition, $s_{|\ker(s-\mathrm{Id}_E)} = \mathrm{Id}_E$ et $s_{|\ker(s+\mathrm{Id}_E)} = -\mathrm{Id}_E$.

Ainsi, s est la symétrie sur $\ker(s - \mathrm{Id}_E)$ parallèlement à $\ker(s + \mathrm{Id}_E)$.

⊠

Remarque : *on peut aussi commencer par montrer (exercice : le faire) que $p = p_{F//G}$ si et seulement si $2p - Id_E = s_{F//G}$ puis déduire le résultat de la caractérisation des projecteurs. En effet, si $s \in \mathcal{L}(E)$ et $p = \frac{1}{2} \cdot (s + Id_E)$ et on a :*

$$s^2 = Id_E \iff p^2 = p$$

Corollaire 4.4.8.20 *Toute symétrie de E est un automorphisme de E.*

Preuve :

On vient de voir qu'une symétrie vérifie $s \circ s = \mathrm{Id}_E$. Par suite, s est une involution de E : c'est donc une bijection.

⊠

Exercice 4.4.8.21 Soit $E = \mathcal{F}(\mathbb{R}, \mathbb{R})$. On considère l'application :

$$\begin{array}{rccc} \varphi : & E & \longrightarrow & E \\ & f & \longmapsto & \varphi(f) \end{array}$$

où pour $f \in E$, on a : $\forall x \in \mathbb{R}$, $\varphi(f)(x) = f(-x)$.

1. Montrer que φ est une symétrie de E.
2. Quel résultat, que vous connaissez déjà, cela permet-il de retrouver ?

Exercice 4.4.8.22 En considérant l'application ψ qui à f associe $x \longmapsto f(x+T)$ retrouver de façon très simple le résultat de l'exercice 4.2.3.8.

Exercice 4.4.8.23 Soient $\mathcal{P}$ le plan d'équation cartésienne $x+y-z=0$ et $\mathcal{D} = \mathbb{R}(1,1,1)$.

1. Montrer que $\mathcal{P} \oplus \mathcal{D} = \mathbb{R}^3$.
2. Soit $s = s_{\mathcal{P}//\mathcal{D}}$. Déterminer l'expression de $s(x,y,z)$ en fonction de x, y, z pour $(x,y,z) \in \mathbb{R}^3$.

4.5 Exercices

Exercice 4.5.1 On se place dans $\mathbb{R}^n$ et on note x_i, pour $1 \leqslant i \leqslant n$ les composantes d'un vecteur. Les ensembles suivants sont-ils des espaces vectoriels ?

$$E_1 = \{x \in \mathbb{R}^2 \ , \ x_1 \in \mathbb{Z}\} \ ; \ E_2 = \{x \in \mathbb{R}^3 \ , \ \sin x_2 = x_1\} \ ; \ E_3 = \{x \in \mathbb{R}^4 \ , \ x_1 = 0\}$$

$$E_4 = \{x \in \mathbb{R}^4 \ , \ x_1 x_2 = 0\} \ ; \ E_5 = \{x \in \mathbb{R}^3 \ , \ x_1 - x_2 = 1\} \ ; \ E_6 = \{x \in \mathbb{R}^3 \ , \ x_1 \neq x_2\}$$

Exercice 4.5.2 Les ensembles suivants sont-ils des sous-espaces vectoriels de $\mathcal{F}(\mathbb{R}, \mathbb{R})$?

$$E_1 = \{f \in E \ , \ f(1) = 0\} \ ; \ E_2 = \{f \in E \ , \ f(-1) = 1\} \ ; \ E_3 = \{f \in E \ , \ f \text{ croissante}\}$$

$$E_4 = \{f \in E \ , \ f \text{ est majorée } \} \quad ; \quad E_5 = \{f \in E \ , \ f(1) = f(2) = f(3) = 0\}$$

$$E_6 = \{f \in E \ , \ f \text{ est monotone}\} \quad ; \quad E_7 = \{f \in E \ , \ \exists a \in \mathbb{R} \ , \ \forall x > a \ , \ f(x) = 0\}$$

Exercice 4.5.3 Les sous-ensembles suivants sont-ils des sous-espaces vectoriels de $\mathbb{R}^{\mathbb{N}}$?

$$E_1 = \{u \in \mathbb{R}^{\mathbb{N}} \ , \ u \text{ monotone}\} \ ; \ E_2 = \{u \in \mathbb{R}^{\mathbb{N}} \ , \ u \text{ converge } \} \ ; \ E_3 = \{u \ , \ u \text{ bornée}\}$$

$$E_4 = \{u \in \mathbb{R}^{\mathbb{N}} \ , \ u \text{ est géométrique}\} \quad ; \quad E_5 = \{u \in \mathbb{R}^{\mathbb{N}} \ , \ u \text{ converge vers } \ell\}$$

$$E_6 = \{u \in \mathbb{R}^{\mathbb{N}} \ . \ u \text{ est arithmétique } \} \quad ; \quad E_7 = \{u \in \mathbb{R}^{\mathbb{N}} \ , \ \sum u_n^2 \text{ converge } \}$$

Exercice 4.5.4 Montrer que $\{f \in \mathcal{F}(\mathbb{R}\cdot\mathbb{R}) \ / \ \exists k_f \in \mathbb{R}^+ \ , \ \forall x \in \mathbb{R} \ , \ |f(x)| \leqslant k_f |x|\}$ est un $\mathbb{R}$-espace vectoriel.

Exercice 4.5.5 Soient F et G deux sous-espaces vectoriels de E. Montrer que :

$$F \cup G \text{ est un sev de } E \iff F \subset G \text{ ou } G \subset F$$

Exercice 4.5.6 Soient E un $\mathbb{K}$-espace vectoriel, A et B deux sous-espaces vectoriels de E. Montrer que $A \cap B = A + B \iff A = B$.

Exercice 4.5.7 Soient A, B et C trois sous-espaces vectoriels de E. Montrer que :

$$A \cap B + A \cap C \subset A \cap (B + C)$$

Donner un exemple où l'inclusion est stricte.

Exercice 4.5.8 Soit E un $\mathbb{R}$-espace vectoriel. Pour $(x, y) \in \mathbb{R}^2$ et $(u, v) \in E^2$, on pose :

$$(x + iy) \cdot (u, v) = (xu - yv, xv + yu)$$

Montrer que E^2 muni de la loi $+$ usuelle et de la loi $\cdot$ définie ci-dessus est un $\mathbb{C}$-espace vectoriel.

Exercice 4.5.9 Soient $c : x \longmapsto \cos(x)$ et $s : x \longmapsto \sin x$. Pour $\varphi \in \mathbb{R}$, on considère la fonction $f_\varphi : x \longmapsto 3\cos(x - \varphi)$. A-t-on $f_\varphi \in Vect(c, s)$?

Exercice 4.5.10 Soient u, v et w les vecteurs de $\mathbb{R}^4$ de coordonnées $(1, 2, 1, 1)$, $(-1, 1, 2, 1)$ et $(5, 4, -1, 1)$. A-t-on $w \in < u, v >$?

Exercice 4.5.11 On note pour $n \in \mathbb{N}$, $c_n : x \longmapsto \cos(nx)$ et $X = \{c_n \ , \ n \in \mathbb{N}\}$.

1. Déterminer une condition nécessaire et suffisante sur $a \in \mathbb{R}$ pour que : $x \longmapsto \cos(ax) \in < X >$.
2. Pour $n \in \mathbb{N}$, est-ce-que $x \longmapsto \cos^n(x) \in < X >$? (On note $\cos^n = (\cos)^n$).
3. Pour quelles valeurs de $n \in \mathbb{N}$ a-t-on $x \longmapsto \sin(x)^n \in < X >$?
4. On note $E = \{f \in \mathcal{C}^0(\mathbb{R}) \ / \ f$ est 2π-périodique et paire $\}$.
   (a) Montrer que E est un espace vectoriel et que $< X >$ est un sous-espace vectoriel de E.
   (b) A-t-on $< X >= E$?

Exercice 4.5.12 Soient A et B deux sous-espaces vectoriels de E, et soit C un supplémentaire de $A \cap B$ dans B. Montrer que $A + B = A \oplus C$.

Exercice 4.5.13 On note $E = \mathcal{F}(\mathbb{R}, \mathbb{R})$ et on considère les ensembles :

$$A = \{f \in E \ / \ f(1) = 0\} \quad \text{et} \quad B = \{f \in E \ / \ \exists a \in \mathbb{R} \ , \ \forall x \in \mathbb{R} \ , \ f(x) = ax\}$$

Montrer que A et B sont des sous-espaces supplémentaires dans E.

Exercice 4.5.14 On considère les ensembles suivants :

$$\begin{aligned} E &= \{(u_n) \in \mathbb{R}^{\mathbb{N}} \mid \forall n \in \mathbb{N} \ , \ u_{n+3} - u_{n+2} - u_{n+1} + u_n = 0\} \\ F &= \{(u_n) \in \mathbb{R}^{\mathbb{N}} \mid \forall n \in \mathbb{N} \ , \ u_{n+1} + u_n = 0\} \\ G &= \{(u_n) \in \mathbb{R}^{\mathbb{N}} \mid \forall n \in \mathbb{N} \ , \ u_{n+2} - 2u_{n+1} + u_n = 0\} \end{aligned}$$

1. Démontrer que E, F et G sont des espaces vectoriels de $\mathbb{R}^{\mathbb{N}}$.
2. Déterminer explicitement les éléments de F et G.
3. Montrer que $F \subset E$ et $G \subset E$.
4. Montrer que $E = F \oplus G$.

Exercice 4.5.15 On considère l'ensemble F suivant :

$$F = \left\{ y \in \mathcal{C}^2(\mathbb{R}, \mathbb{R}) \ / \ \forall x \in \mathbb{R} \ , \ y''(x) = (1 + x^2)y(x) \right\}$$

1. Montrer que F est un $\mathbb{R}$-espace vectoriel.
2. On considère les fonctions suivantes définies pour tout réel x par :

$$f(x) = \exp\left(\frac{x^2}{2}\right) \quad \text{et} \quad g(x) = f(x) \int_0^x e^{-t^2} \, \mathrm{d}t$$

   (a) Montrer que f et g appartiennent à F.

   (b) Montrer que si u et v sont deux fonctions qui sont dans F, alors la fonction $W = uv' - u'v$ est constante [1].

   (c) Si h appartient à F, comparer les dérivées de $\dfrac{h}{f}$ et $\dfrac{g}{f}$.

   (d) En déduire que $F = \mathrm{Vect}(f, g)$.

Exercice 4.5.16 On considère l'espace vectoriel $E = \mathcal{F}(\mathbb{R}, \mathbb{R})$ ainsi que les ensembles :

$$F = \{f \in E \ / \ f \text{ est de période } 1\} \quad \text{et} \quad G = \{f \in E \ / \ \lim_{x \to +\infty} f(x) = 0\}$$

1. Démontrer que F et G sont des sous-espaces vectoriels de E.
2. Démontrer que F et G sont en somme directe *(On pourra penser à utiliser une suite qui tend vers l'infini).*
3. F et G sont-ils supplémentaires dans E ?

Exercice 4.5.17 Parmi les applications suivantes de $\mathbb{R}^2$ dans $\mathbb{R}^2$, lesquelles sont des applications linéaires ?

$$f_1 : (x, y) \mapsto (2x + y, -2x - y) \quad ; \quad f_2 : (x, y) \mapsto (x + 1, y) \quad ; \quad f_3 : (x, y) \mapsto (0, x)$$

$$f_4 : (x, y) \mapsto (x^2, y) \quad ; \quad f_5 : (x, y) \mapsto (y, x) \quad ; \quad f_6 : (x, y) \mapsto (|x|, y)$$

Exercice 4.5.18 Pour chacune des applications suivantes, dire s'il s'agit d'une application linéaire. Si oui, préciser son image et son noyau. En déduire alors si l'application est injective, surjective.

1. L'application f de $\mathbb{R}^2$ dans $\mathbb{R}^2$ qui à (x, y) associe $(-x + 2y, x + y)$.
2. L'application g de $\mathcal{C}^\infty(R)$ dans lui-même, qui à une fonction y associe $y' + xy$.
3. L'application h de $\mathcal{B}(\mathbb{N}, R)$ dans $\mathbb{R}$ qui à (u_n) associe $\sup_{n \in \mathbb{N}} u_n$.
4. L'application T de $\mathbb{R}^3$ dans $\mathbb{R}^2$ qui à (x, y, z) associe $(x - z, y - z)$.
5. L'application P de $\mathbb{R}$ dans $\mathbb{R}^3$ qui à x associe $(x, 1 + x, 2x)$.

1. Pour information, la fonction W est le Wronskien des deux solutions u et v.

Exercice 4.5.19 Soit $E = \mathbb{R}^3$ muni de sa base canonique $(\vec{i}, \vec{j}, \vec{k})$.

1. Montrer qu'il existe un unique endomorphisme u de E tel que :
$$u(\vec{i}) = -\sqrt{2}\vec{i} + \vec{k} \quad \text{et} \quad u(\vec{j}) = \sqrt{2}\vec{j} + \vec{k} \quad \text{et} \quad u(\vec{k}) = \vec{i} + \vec{j}$$
2. Déterminer le noyau de u.
3. Déterminer l'ensemble F des vecteurs $\vec{x}$ de E tels que $u(\vec{x}) = 2\vec{x}$.
4. Déterminer l'ensemble G des vecteurs $\vec{x}$ tels que $u(\vec{x}) = -2\vec{x}$.

Exercice 4.5.20 On se place dans $E = \mathbb{R}^3$ et on note $(\vec{i}, \vec{j}, \vec{k})$ la base canonique de E. On note $\vec{v} = \vec{i} - \vec{j} + \vec{k}$ et on désigne par f, l'application qui à $\vec{x}$ de coordonnées (x, y, z) associe :
$$f(\vec{x}) = \vec{x} - 2(x + y + z)\vec{v}$$
1. Montrer que f est un endomorphisme de E.
2. Déterminer f^2.
3. En déduire que f est bijective et donner f^{-1}, $\ker(f)$ et $\mathrm{Im}(f)$.
4. Montrer que $\ker(f - \mathrm{Id}_E) \oplus \ker(f + \mathrm{Id}_E) = E$ et déterminer une base de chacun de ces espaces.
5. Déterminer $\mathrm{Im}(f - \mathrm{Id}_E)$ et $\mathrm{Im}(f + \mathrm{Id}_E)$.

Exercice 4.5.21 On considère les ensembles F et G suivants :
$$F = \{(x, y, z) \in \mathbb{R}^3 \ / \ y = z\}$$
$$G = \{(x, y, z) \in \mathbb{R}^3 \ / \ x - y = 0 \text{ et } z - 2y = 0\}$$
1. Montrer que F et G sont des sous-espaces vectoriels de $\mathbb{R}^3$.
2. Montrer que F est un plan et déterminer une base de F.
3. Montrer que G est une droite vectorielle et donner un vecteur directeur de G.
4. Montrer que F et G sont supplémentaires dans $\mathbb{R}^3$.
5. Soit p le projecteur sur F parallèlement à G. Déterminer l'expression de $p(x, y, z)$, pour $(x, y, z) \in \mathbb{R}^3$.
6. Soit q l'endomorphisme de $\mathbb{R}^3$ défini par :
$$\begin{array}{rccc} q : & \mathbb{R}^3 & \longrightarrow & \mathbb{R}^3 \\ & (x, y, z) & \longrightarrow & (x + y - z, y, y) \end{array}$$
On admet donc que q est un endomorphisme de $\mathbb{R}^3$. Montrer que q est un projecteur.

7. Montrer que $\ker(q)$ est une droite vectorielle.
8. Vérifier que $\ker(q)$ et G sont en somme directe.
9. Montrer que $\mathrm{Im}(q) = F$.
10. En déduire que $p \circ q = q$ et que $q \circ p = p$ (*il n'est pas nécessaire d'avoir calculé p à la question 5 pour répondre à cette question et aux suivantes*).
11. On pose $r = p + q$. Est-ce que r est un projecteur ?
12. Pour tout entier $n \geqslant 2$ calculer r^n en fonction de r.
13. Montrer les deux inclusions :

$$(a)\ \mathrm{Im}(r - 2\mathrm{Id}_{\mathbb{R}^3}) \subset \ker(r) \quad \text{et} \quad (b)\ \mathrm{Im}(r) \subset \ker(r - 2\mathrm{Id}_{\mathbb{R}^3})$$

14. Montrer que $\mathbb{R}^3 = \ker(r) \oplus \ker(r - 2\mathrm{Id}_{\mathbb{R}^3})$.
15. Donner l'expression (en fonction de $x, y, z) \in \mathbb{R}^3$) de la symétrie s par rapport à $\ker(r)$ parallèlement à $\ker(r - 2\mathrm{Id}_{\mathbb{R}^3})$.

Exercice 4.5.22 Soient E, F et G trois $\mathbb{K}$-ev. On suppose que $f \in \mathcal{L}(E, F)$, f surjective, $g : F \longrightarrow G$ est une application et que $g \circ f$ est linéaire. Montrer que g est linéaire.

Exercice 4.5.23 Soit E un espace vectoriel et $f \in \mathcal{L}(E)$. Montrer les équivalences suivantes :

1. $E = \ker(f) + \mathrm{Im}(f) \iff \mathrm{Im}(f) = \mathrm{Im}(f^2)$.
2. $\mathrm{Im}(f) \cap \ker(f) = \{0\} \iff \ker(f) = \ker(f^2)$.

Exercice 4.5.24 Soient E, F et G trois $\mathbb{K}$-espaces vectoriels, $f \in \mathcal{L}(E, F)$ et $g \in \mathcal{L}(F, G)$.

1. Montrer que : $\ker(g \circ f) = \ker(f) \iff \ker(g) \cap \mathrm{Im}(f) = \{0\}$.
2. Montrer aussi que : $\mathrm{Im}(g \circ f) = \mathrm{Im}(g) \iff \ker(g) + \mathrm{Im}(f) = F$.

Exercice 4.5.25 On considère E, F et G trois $\mathbb{K}$-espaces vectoriels, $f \in \mathcal{L}(E, F)$ ainsi que $g, h \in \mathcal{L}(F, G)$. Montrer que :

$$\ker(g \circ f) = \ker(h \circ f) \iff \mathrm{Im}(f) \cap \ker(g) = \mathrm{Im}(f) \cap \ker(h)$$

Exercice 4.5.26 Soit E un $\mathbb{K}$-espace vectoriel et p un projecteur de E. On suppose que $\lambda \in \mathbb{K} \setminus \{0, 1\}$. Montrer que $p - \lambda\mathrm{Id}_E$ est un automorphisme de E :

1. en cherchant un inverse sous la forme $ap + b\mathrm{Id}_E$ avec $(a, b) \in \mathbb{K}^2$;
2. en prouvant directement que $p - \lambda\mathrm{Id}_E$ est bijective.

Exercice 4.5.27 Soient E un $\mathbb{K}$-espace vectoriel, p et q deux projecteurs de E. Montrer que :

$$p+q \text{ est un projecteur} \iff p\circ q = q\circ p = 0$$

Indication : pour l'implication directe, on pourra montrer que $pq+qp=0$ puis montrer que $pq=qp$.

Montrer qu'alors $\mathrm{Im}(p+q) = \mathrm{Im}(p)\oplus\mathrm{Im}(q)$ et que $\ker(p+q) = \ker(p)\cap\ker(q)$.

Exercice 4.5.28 Soient E un $\mathbb{K}$-espace vectoriel et $f,g\in\mathcal{L}(E)$. Démontrer l'équivalence des deux propriétés suivantes :

(*i*) $f\circ g = g$ et $g\circ f = f$;

(*ii*) f et g sont des projecteurs de E et $\mathrm{Im}(f) = \mathrm{Im}(g)$.

Exercice 4.5.29 Soit E un $\mathbb{K}$-espace vectoriel. Soient par ailleurs A et B deux sous-espaces vectoriels de E, supplémentaires dans E. On pose :

$$G = \{f\in\mathcal{L}(E) \ / \ \ker(f) = A \quad \text{et} \quad \mathrm{Im}(f) = B\}$$

1. Soit $f\in G$. Montrer que B est stable par f, c'est-à-dire que $\forall x\in B$, $f(x)\in B$.
2. Montrer alors que si $f\in G$, alors $f_{|B}$ est un automorphisme de B.
3. Démontrer que G est un groupe pour la loi $\circ$ et qu'il est isomorphe à $\mathcal{GL}(B)$.
4. G est-il un sous-groupe de $\mathcal{GL}(E)$?

Exercice 4.5.30 Dans cet exercice, on étudie les endomorphismes annulés par un polynôme du second degré scindé à racines simples et quelques applications.

Partie 1 : généralités

Soit E un $\mathbb{K}$-espace vectoriel. On considère également α,β deux éléments distincts de $\mathbb{K}$ et $f\in\mathcal{L}_{\mathbb{K}}(E)$ tel que :

$$(f-\alpha\mathrm{Id}_E)\circ(f-\beta\mathrm{Id}_E) = 0$$

1. Montrer qu'on a aussi : $(f-\beta\mathrm{Id}_E)\circ(f-\alpha\mathrm{Id}_E) = 0$.

   On pose pour la suite $F_\alpha = \ker(f-\alpha Id_E)$ et $F_\beta = \ker(f-\beta Id_E)$.
2. Montrer que F_α et F_β sont des $\mathbb{K}$-espaces vectoriels.
3. Démontrer que : $\mathrm{Im}(f-\beta\mathrm{Id}_E)\subset F_\alpha$ et $\mathrm{Im}(f-\alpha\mathrm{Id}_E)\subset F_\beta$.
4. Montrer que F_α et F_β sont supplémentaires dans E.
5. On appelle p la projection sur F_α parallèlement à F_β et q le projecteur associé à p. Établir que :

$$p+q = \mathrm{Id}_E \quad \text{et} \quad p\circ q = q\circ p = 0$$

6. Montrer que $f = \alpha p + \beta q$ et en déduire l'expression de f^n pour $n \in \mathbb{N}$ en fonction de α, β, p et q.
7. On suppose que $f \notin < \mathrm{Id}_E >$. Prouver que f est bijective si et seulement si $\alpha\beta \neq 0$ et exprimer dans ce cas f^{-1} en fonction de α, β, p et q puis plus généralement, f^n lorsque $n \in \mathbb{Z}$.

Partie 2 : étude d'un exemple

On considère l'application f de $\mathbb{R}^2$ dans lui-même définie pour tout $(x, y) \in \mathbb{R}^2$ par :

$$f(x, y) = (-2x + y, x - 2y)$$

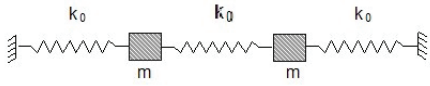
1. Démontrer que f est un endomorphisme de $\mathbb{R}^2$.
2. f est-il un automorphisme de $\mathbb{R}^2$?
3. Calculer pour $(x, y) \in \mathbb{R}^2$, $(f \circ f)(x, y)$.
4. En déduire l'existence de deux réels $\alpha < \beta$, que vous déterminerez, tels que :

$$(f - \alpha \mathrm{Id}_{\mathbb{R}^2}) \circ (f - \beta \mathrm{Id}_{\mathbb{R}^2}) = 0$$

5. Déterminer alors les sous-espaces vectoriels F_α et F_β. Pour chacun, on donnera une équation cartésienne ainsi qu'une base.
6. Calculer explicitement pour $(x, y) \in \mathbb{R}^2$, $p(x, y)$ et $q(x, y)$ (où p et q sont les projecteurs définies dans la première partie mais pour cette application f).
7. Vérifier que $p + q = \mathrm{Id}_{\mathbb{R}^2}$ et que $p \circ q = q \circ p = 0$.
8. Déterminer l'endomorphisme f^n pour $n \in \mathbb{Z}$ (donner explicitement $f^n(x, y)$ pour $(x, y) \in \mathbb{R}^2$).

Partie 3 : application

Deux masses identiques sont reliées à deux points fixes et entre elles par trois ressorts de même raideur k_0. On choisit k_0 et m de sorte que $\frac{k_0}{m} = 1$ (s^{-2}) :



On admet que les abscisses x_1 et x_2 des deux masses, repérées par rapport à leurs positions d'équilibre respectives, sont solutions du système différentiel suivant :

$$\begin{cases} \ddot{x}_1 &= -2x_1 + x_2 \\ \ddot{x}_2 &= x_1 - 2x_2 \end{cases}$$

1. Prouver que pour tout réel t, $(\ddot{x}_1(t), \ddot{x}_2(t)) = f(x_1(t), x_2(t))$, où f est l'endomorphisme défini dans la seconde partie.

2. On note $\vec{u}$ (respectivement $\vec{v}$), un vecteur directeur de F_α (respectivement F_β) (voir partie 2).

   (a) Justifier qu'il existe deux fonctions a et b telles que :

   $$\forall t \in \mathbb{R} \ , \ (x_1(t), x_2(t)) = a(t)\vec{u} + b(t)\vec{v}$$

   (b) Montrer que les fonctions a et b sont deux fois dérivables sur $\mathbb{R}$.

   (c) Établir que :

   $$\forall t \in \mathbb{R} \ , \ \ddot{a}(t)\vec{u} + \ddot{b}(t)\vec{v} = \alpha a(t)\vec{u} + \beta b(t)\vec{v}$$

   (d) En déduire que a et b sont solutions d'une équation différentielle linéaire du second ordre à coefficients constants.

   (e) Résoudre cette équation et en déduire les solutions du système différentiel proposé.

3. Déterminer la solution du système proposé vérifiant les conditions initiales suivantes :

   $$x_1(0) = 0 \ ; \ \dot{x}_1(0) = 1 \ ; \ x_2(0) = 1 \ ; \ \dot{x}_2(0) = 0$$

Chapitre 5

Arithmétique dans $\mathbb{Z}$

Prérequis : dans tout ce chapitre, les notions suivantes sont supposées connues :

- le cours de logique (implications, équivalences, prédicat) ;
- relation d'équivalence, relation d'ordre, plus petit et plus grand élément ;
- l'ensemble $\mathbb{N}$ et toutes ses propriétés ;
- la structure d'anneau $(\mathbb{Z}, +, \times)$ et les propriétés de l'ensemble ordonné $(\mathbb{Z}, \leqslant)$;
- groupes, anneaux et corps, morphismes de groupes ou d'anneaux.

Aucune connaissance spécifique en arithmétique n'est supposée connue.

5.1 Arithmétique dans $\mathbb{Z}$

5.1.1 Diviseurs et congruences

Définition 5.1.1.1 Soit $(a,b) \in \mathbb{Z}^2$. On dit que a divise b, et on note alors $a|b$, si $\exists c \in \mathbb{Z}$, $b = ac$.

Remarques et notation :

- *on peut aussi dire que b est un multiple de a, ou encore que a est un diviseur de b. On note alors $a\mathbb{Z}$ l'ensemble des multiples de a, c'est-à-dire :*
$$a\mathbb{Z} = \{na \ , \ n \in \mathbb{Z}\}$$
- $\forall b \in \mathbb{Z}$, $1|b$ *puisque pour tout $b \in \mathbb{Z}$, il existe $c = b \in \mathbb{Z}$ tel que $b = 1 \times b = 1 \times c$;*
- $\forall a \in \mathbb{Z}$, $a|0$ *et* $a|a$ *;*
- *pour tout $a \in \mathbb{Z}$, $0|a \iff a = 0$;*
- *si $n|a$ et $n|b$, alors pour tout $(u,v) \in \mathbb{Z}^2$, $n|ua + vb$;*
- $a|b$ *si et seulement si* $b\mathbb{Z} \subset a\mathbb{Z}$.

Proposition 5.1.1.2 *La relation $|$ est réflexive et transitive mais n'est pas antisymétrique. Plus exactement,*
$$\forall (a,b) \in \mathbb{Z}^2 \ , \ \Big((a|b \ \text{ et } \ b|a) \iff |a| = |b| \Big)$$

Preuve :

• On a vu que pour tout $a \in \mathbb{Z}$, $a|a$. Par suite, $|$ est réflexive.

• Par ailleurs, soient $a, b, c \in \mathbb{Z}$ tels que $a|b$ et $b|c$: il existe $n, p \in \mathbb{Z}$ tels que $b = na$ et $c = pb$. Alors $c = pna = (np)a$ avec $np \in \mathbb{Z}$. Par suite, $a|c$ et la relation $|$ est transitive.

• Enfin, si $a, b \in \mathbb{Z}$ vérifient $a|b$ et $b|a$, alors il existe deux entiers relatifs n et p tels que $a = nb$ et $b = pa$. Il s'ensuit que $a = npa$, soit encore $a(np - 1) = 0$. L'anneau $\mathbb{Z}$ étant intègre, il y a deux cas :

  ∗ soit $a = 0$, et dans ce cas, on a $b = pa = 0$ donc $|a| = |b| = 0$;
  ∗ ou bien $np = 1$ et puisque $n, p \in \mathbb{Z}$, $n = p = 1$ ou $n = p = -1$, c'est-à-dire $a = b$ ou $a = -b$, soit encore $|a| = |b|$.

Réciproquement, il est clair que si $|a| = |b|$, alors $a|b$ et $b|a$. ⊠

Définition 5.1.1.3 Soient $n \in \mathbb{N}^\star$ et $(a,b) \in \mathbb{Z}^2$. On dit que a est congru à b modulo n, et on note $a \equiv b \ \ [n]$, si $n|(b-a)$.

Remarque : *par définition, si* $n \in \mathbb{N}^\star$, $a \equiv b \ \ [n] \iff \exists k \in \mathbb{Z}$, $b = a + kn$.

Proposition 5.1.1.4 *Pour* $n \in \mathbb{N}^\star$ *fixé, la relation de congruence modulo* n, $\equiv$, *est une relation d'équivalence. De plus, elle est compatible avec l'addition et la multiplication :*

$$\forall a,b,c,d \in \mathbb{Z} \ , \ (a \equiv b \ \ [n] \ \textit{et} \ c \equiv d \ \ [n] \implies a + c \equiv b + d \ \ [n] \ \textit{et} \ ac \equiv bd \ \ [n] \ )$$

Preuve :

• Montrons pour commencer que $\equiv$ est une relation d'équivalence.

∗ Montrons que $\equiv$ est réflexive.
Pour tout $a \in \mathbb{Z}$, $n|0$, soit encore $n|(a-a)$. Par suite, $a \equiv a \ \ [n]$ et la relation $\equiv$ est donc réflexive.

∗ Montrons que $\equiv$ est symétrique.
Soient $a \in \mathbb{Z}$ et $b \in \mathbb{Z}$ tels que $a \equiv b \ \ [n]$. Par définition, $n|(b-a)$, c'est-à-dire qu'il existe $c \in \mathbb{Z}$ tel que $b - a = cn$. Mais alors, $a - b = (-c) \times n$ donc $n|(a-b)$, c'est-à-dire $b \equiv a \ \ [n]$. Ce qui prouve que $\equiv$ est symétrique.

∗ Enfin, montons que $\equiv$ est transitive.
Soit $(a,b,c) \in \mathbb{Z}^3$ tel que $a \equiv b \ \ [n]$ et $b \equiv c \ \ [n]$. Alors, n divise $b - a$ et n divise $c - b$. Par suite, il existe $k, l \in \mathbb{Z}$ tels que : $b - a = kn$ et $c - b = ln$. En additionnant, on obtient : $c - a = (k + l)n$ et donc $a \equiv c \ \ [n]$. D'où la transitivité.

Ce qui prouve que $\equiv$ est bien une relation d'équivalence sur $\mathbb{Z}$.

• Montrons à présent la compatibilité avec l'addition et la multiplication.
Soit $(a,b,c,d) \in \mathbb{Z}^4$ tel que $a \equiv b \ \ [n]$ et $c \equiv d \ \ [n]$. Il existe $k, l \in \mathbb{Z}$ tels que $b = a + kn$ et $d = c + ln$. En additionnant, on a directement : $b + d = a + c + (k + l)n$, c'est-à-dire $a + c \equiv b + d \ \ [n]$.
Pour la multiplication, on remarque que :

$$ac - bd = ac - bc + bc - bd = (a - b)c + b(c - d)$$

Or, $n|(a-b)$ et $n|(c-d)$ donc $n|\left((a-b)c + b(c-d)\right)$ et $ac \equiv bd \ \ [n]$.

⊠

⚠ **Attention :** on ne peut pas diviser ou simplifier en général ! Par exemple,

$$2 \times 6 \equiv 2 \times 2 \ \ [8] \qquad \text{mais} \quad 6 \not\equiv 2 \ \ [8]$$

Il faut donc manipuler les congruences (c'est-à-dire le symbole $\equiv$) avec attention. On verra un peu plus loin dans quels cas on peut simplifier. Si vous avez le moindre doute, écrivez la congruence sous forme d'une égalité et regardez s'il est possible de simplifier (ou non) dans l'égalité.

Corollaire 5.1.1.5 *Soient $n \in \mathbb{N}^\star$ et $(a,b) \in \mathbb{Z}^2$. Alors :*

$$a \equiv b \ \ [n] \implies \big(\forall k \in \mathbb{N} \ , \ a^k \equiv b^k \ \ [n] \ \big)$$

Preuve :

On suppose que $a \equiv b \ \ [n]$.

• Avec les conventions usuelles, $a^0 = b^0 = 1$ donc $a^0 \equiv b^0 \, [n]$. La propriété est donc vraie au rang 0.

• Montrons par récurrence que $\forall k \in \mathbb{N}^\star$, $a^k \equiv b^k \, [n]$.

Initialisation :

Pour $k = 1$, $a \equiv b \ \ [n]$ par hypothèse. La propriété est donc vraie au rang $k = 1$.

Hérédité :

On suppose la propriété vraie au rang $k \geqslant 1$: montrons qu'elle est vraie au rang $k+1$. Par hypothèse de récurrence, $a^k \equiv b^k \ \ [n]$ et on a aussi $a \equiv b \ \ [n]$. La relation de congruence étant compatible avec la multiplication, on a donc :

$$a \times a^k \equiv b \times b^k \ \ [n] \qquad \text{c'est-à-dire} \qquad a^{k+1} \equiv b^{k+1} \ \ [n]$$

Ce qui montre que la propriété est vraie au rang $k+1$ et achève la récurrence. ⊠

Exercice 5.1.1.6 Quel est le dernier chiffre dans l'écriture en base 4 de l'entier naturel $N = 106 \times 2011^{2011} - 59 \times 2006^{2011}$? Et en base 10 ?

Exercice 5.1.1.7 Proposer une autre preuve directe en utilisant la factorisation de $b^k - a^k$ (voir proposition 1.2.3.9).

5.1.2 Nombres premiers et décomposition en produit de facteurs premiers

Définition 5.1.2.1 Un nombre entier naturel p est dit premier s'il admet exactement deux diviseurs (dans $\mathbb{N}$) qui sont 1 et p.
Un nombre entier qui n'est pas premier est dit composé.

Exemple 5.1.2.2 Les nombres $2, 3, 5, 7, 11, 13, 17, 19, 23, 29$ sont des nombres premiers.

Exemple 5.1.2.3 Les nombres $4, 121, 221$ sont des nombres composés.

⚠ **Attention :** 1 n'est pas premier puisqu'il n'admet qu'un seul diviseur dans $\mathbb{N}$.

Théorème 5.1.2.4 *Tout entier naturel $n \geqslant 2$ admet au moins un diviseur premier.*

Preuve :

On montre le résultat par récurrence forte.

Initialisation :

Pour $n = 2$, n est divisible par 2 qui est bien premier. La propriété est vraie au rang $n = 2$.

Hérédité :

On suppose que la propriété est vraie pour tout entier $k \in [\![2, n]\!]$ pour un certain entier $n \geqslant 2$. Montrons qu'elle est vraie au rang $n + 1$. On a alors deux cas :

- si $n + 1$ est premier, alors $n + 1$ est divisible par $n + 1$ qui est premier ;
- si $n+1$ n'est pas premier, alors $n+1$ admet un diviseur a différent de 1 et de $n+1$, c'est-à-dire qu'il existe b tel que $n+1 = ab$ avec $2 \leqslant a \leqslant n$. Par hypothèse de récurrence, a admet au moins un diviseur premier p. Ce nombre premier p est alors un diviseur de $n + 1$.

Ce qui montre que la propriété est vraie au rang $n + 1$ et achève la récurrence.

⊠

Proposition 5.1.2.5 *Un entier naturel $n \geqslant 2$ est composé si et seulement si il admet un diviseur premier p tel que $p \leqslant \sqrt{n}$.*

Preuve :

• Montrons $\Longrightarrow$

Soit $n \geqslant 2$ un nombre composé. Alors il existe deux entiers naturels a et b tels que $n = ab$, $1 < a < n$ et $1 < b < n$. Par ailleurs, il est clair que $a \leqslant \sqrt{n}$ ou bien $b \leqslant \sqrt{n}$. En effet, dans le cas contraire, $a > \sqrt{n}$ et $b > \sqrt{n}$ et par conséquent, $ab > n$: ce qui est absurde.
Quitte à échanger les noms, on peut supposer que $a \leqslant \sqrt{n}$. Sachant que $a \geqslant 2$, on peut appliquer le théorème précédent, et a admet un diviseur premier p. Il est alors clair que $p|n$ et $p \leqslant \sqrt{n}$.

• Réciproquement, si $n \geqslant 2$ admet un diviseur premier tel que $p \leqslant \sqrt{n}$, alors ce diviseur p est strictement plus grand que 1 (puisque 1 n'est pas premier) et strictement inférieur à n (puisque $\sqrt{n} < n$ pour $n \geqslant 2$). Ainsi, n n'est pas premier car il admet un diviseur autre que 1 ou n.

⊠

▶ Méthode : Pour montrer qu'un nombre entier naturel $n \geqslant 2$ est premier, il faut et il suffit de prouver qu'il n'est divisible par aucun nombre premier $p \leqslant \sqrt{n}$.

Exemple 5.1.2.6 Montrons que 1009 est premier. Puisque $31 < \sqrt{1009} < 32$, il faut et il suffit de prouver que 1009 n'est pas divisible par un nombre premier plus petit que 32, c'est-à-dire n'est pas divisible par 2, 3, 5, 7, 11, 13, 17, 19, 23, 29 et 31. Pour 2, 3 et 5, on connaît les critères pratiques et c'est donc facile de vérifier qu'ils ne divisent pas 1009. Pour les autres, on peut faire la division euclidienne (voir paragraphe suivant) ou utiliser les calculs de congruences. Par exemple,

$$1009 \equiv 1009 - 31 \times 30 \ [31] \equiv 709 \ [31] \equiv 709 - 31 \times 22 \ [31] \equiv 27 \ [31] \not\equiv 0 \ [31]$$

Théorème 5.1.2.7 *L'ensemble des nombres premiers est infini.*

Preuve :

Voir le cours de logique (ou refaire la preuve en raisonnant par l'absurde et en considérant un facteur premier de $N = \prod_{p \in \mathcal{P}} p + 1$).

⊠

Théorème 5.1.2.8 (Décomposition en facteurs premiers) *Tout entier naturel $n \geqslant 2$ se décompose de façon unique (à l'ordre près) en produit de nombres premiers. Autrement dit, n s'écrit sous la forme :*

$$n = \prod_{i=1}^{r} p_i^{\alpha_i}$$

où $r \in \mathbb{N}^\star$ et pour tout $i \in [\![1, r]\!]$, p_i est premier et $\alpha_i \in \mathbb{N}^\star$ et les p_i sont deux à deux distincts. De plus, cette écriture est unique à l'ordre près des facteurs.

Preuve :

On a déjà prouvé l'existence (voir exemple 2.2.2.8 sur l'ensemble $\mathbb{N}$). On montrera l'unicité (à l'ordre près) un peu plus loin dans le cours.

⊠

Remarques :

- *avec la convention qu'un produit vide est égal à 1, le théorème reste valable pour $n = 1$ qui est le produit vide de nombres premiers ;*
- *dans la pratique, trouver la décomposition en facteurs premiers est un problème difficile et c'est sur cela que repose de nombreuses méthodes de cryptographie.*

Définition 5.1.2.9 On dit que $p \in \mathbb{Z}$ est premier si $|p|$ est un entier naturel qui est premier.

Remarque : *de façon équivalente, $p \in \mathbb{Z}$ est premier si et seulement si p admet exactement 4 diviseurs dans $\mathbb{Z}$ qui sont 1, -1, p et $-p$.*

Corollaire 5.1.2.10 *Tout entier relatif $n \notin \{-1, 0, 1\}$ s'écrit sous la forme :*

$$n = \pm \prod_{i=1}^{r} p_i^{\alpha_i}$$

où $r \in \mathbb{N}^\star$ et pour tout $i \in [\![1, n]\!]$, $p_i \in \mathbb{N}$ est premier, $\alpha_i \in \mathbb{N}^\star$ et les p_i sont deux à deux distincts. De plus, cette écriture est unique à l'ordre près des facteurs.

5.1.3 Division euclidienne

Théorème 5.1.3.1 (Division euclidienne) *Soient $a \in \mathbb{Z}$ et $b \in \mathbb{N}^\star$. Alors il existe un unique couple $(q, r) \in \mathbb{Z}^2$ tel que :*

$$a = qb + r \quad \text{et} \quad 0 \leqslant r < b$$

q est appelé le quotient de la division euclidienne de a par b et r le reste.

Preuve :

• Montrons l'existence.

Considérons $A = \{n \in \mathbb{Z} \ , \ nb \leqslant a\}$. A est une partie de $\mathbb{Z}$ qui est :

- non vide (elle contient 0 si $a \geqslant 0$ et a si $a < 0$) ;
- et majorée (par a si $a \geqslant 0$ et par 0 sinon).

Par conséquent, A possède un plus grand élément. Notons le q et posons $r = a - qb$. Par définition, $q \in A$ donc $qb \leqslant a$, soit encore $r \geqslant 0$. Enfin, $(q+1) \notin A$, donc $(q+1)b > a$, soit encore $r < b$.

• Montrons l'unicité.

Soient (q, r) et (q', r') deux tels couples. Alors : $qb + r = q'b + r'$, soit $r' - r = b(q - q')$. Or, $0 \leqslant r' < b$ et $-b < -r \leqslant 0$. Par conséquent, $r' - r \in b\mathbb{Z}$ et $-b < r' - r < b$. Par suite, $r' - r = 0$, c'est-à-dire $r = r'$ et en remplaçant, on obtient $q = q'$. D'où l'unicité. ⊠

Remarques :

- *on pouvait aussi chercher à caractériser q directement en utilisant les rationnels et la fonction partie entière. En effet, $q = E\left(\frac{a}{b}\right)$;*
- *la division euclidienne est un outil important pour le calcul de pgcd (voir paragraphe 6) ;*
- *on verra aussi dans le chapitre sur les polynômes que la division euclidienne peut se généraliser à d'autres anneaux que $\mathbb{Z}$ (mais pas tous les anneaux) ;*
- *avec les hypothèses et notations du théorème $b|a$ si et seulement si le reste de la division euclidienne de a par b est nul ;*
- *dans la pratique, quand a et b sont « grands », on fait des divisions successives (mais pas euclidiennes) jusqu'à obtenir un reste qui est bien dans $[\![0, b-1]\!]$;*
- *le reste r est caractérisé par $a \equiv r \ \ [b]$ et $r \in [\![0, b-1]\!]$. Le calcul du reste est en général plus simple que celui du quotient.*

5.1.4 Sous-groupes de $(\mathbb{Z}, +)$

Théorème 5.1.4.1 *Les sous-groupes de $(\mathbb{Z}, +)$ sont les $n\mathbb{Z}$, avec $n \geqslant 0$.*

Preuve :

• Montrons que pour tout $n \in \mathbb{N}$, $n\mathbb{Z}$ est un sous-groupe de $(\mathbb{Z}, +)$.

Soit $n \in \mathbb{N}$ et soit $\varphi_n : \mathbb{Z} \longrightarrow \mathbb{Z}$ définie par : $\forall x \in \mathbb{Z}$, $\varphi_n(x) = nx$.
La multiplication dans $\mathbb{Z}$ étant distributive par rapport à l'addition, φ_n est un morphisme de groupes. Par conséquent, $n\mathbb{Z} = \mathrm{Im}(\varphi_n)$ est un sous-groupe de $\mathbb{Z}$.

• Réciproquement, soit H un sous-groupe de $(\mathbb{Z}, +)$.
Si $H = \{0\}$, alors $H = 0\mathbb{Z}$ et le résultat est prouvé.
On suppose donc que $H \neq \{0\}$. Il existe alors $x \in H$ tel que $x \neq 0$. H étant un sous-groupe, il est stable par opposé : $-x \in H$. Par suite, $\{-x, x\} \subset H$, et donc $|x| \in H \cap \mathbb{N}^\star$.

Ainsi, $H \cap \mathbb{N}^\star$ est une partie non vide de $\mathbb{N}$: elle admet donc un plus petit élément. Soit $n = \min(H \cap \mathbb{N}^\star)$. Montrons que $H = n\mathbb{Z}$.

- ∗ Par définition du plus petit élément, $n \in H$. Puisque H est un sous-groupe de $\mathbb{Z}$, on en déduit immédiatement que $n\mathbb{Z} \subset H$ (on peut par exemple prouver par récurrence immédiate que $kn \in H$ pour tout $k \in \mathbb{N}$ puis la stabilité par opposé donne le résultat pour $k \in \mathbb{Z}$).
- ∗ Réciproquement, soit $h \in H$. On effectue la division euclidienne de h par n (licite puisque $n \in \mathbb{N}^\star$) : il existe un unique couple $(q, r) \in \mathbb{Z}^2$ tel que $h = qn + r$ et $0 \leqslant r < n$.
  Or, on sait que $h \in H$ et d'après ce qui précède, $qn \in n\mathbb{Z} \subset H$. H étant un sous-groupe de $\mathbb{Z}$, $h - nq \in H$, c'est-à-dire $r \in H$. Enfin,
  $$\left\{ \begin{array}{l} r \in H \\ 0 \leqslant r < n \\ n = \min(H \cap \mathbb{N}^\star) \end{array} \right. \quad \Longrightarrow r = 0$$
  Par conséquent, $h = qn \in n\mathbb{Z}$.

Ainsi, on a montré par double inclusion que $H = n\mathbb{Z}$.

⊠

On va voir dans les paragraphes suivants que ce théorème est très important et permet d'établir des relations fondamentales en arithmétique !

5.1.5 Plus grand commun diviseur et plus petit commun multiple

Proposition 5.1.5.1 (Définition) *Soient a et b deux entiers relatifs.*

(i) On suppose que $(a,b) \neq (0,0)$. L'ensemble des diviseurs communs de a et b admet un plus grand élément. Ce plus grand élément est appelé le plus grand commun diviseur de a et b, et est noté $pgcd(a,b)$, ou parfois $a \wedge b$.

(ii) On suppose a et b non nuls. L'ensemble des multiples communs de a et b admet un plus petit élément strictement positif : cet élément est appelé le plus petit commun multiple de a et b, et est noté $ppcm(a,b)$ ou parfois $a \vee b$.

Preuve :

(*i*) Notons $D(a,b) = \{n \in \mathbb{Z} \ / \ n|a \text{ et } n|b\}$. $D(a,b)$ est une partie de $\mathbb{Z}$ qui est non vide (car $1 \in D(a,b)$) et majorée (par $|a|$ par exemple). Par conséquent, elle admet un plus grand élément.

(*ii*) De la même façon, notons $M(a,b) = \{n \in \mathbb{Z} \ / \ a|n \text{ et } b|n\}$. Alors, $M(a,b) \cap \mathbb{N}^\star$ est une partie de $\mathbb{N}$ qui est non vide (elle contient $|ab|$ par exemple). Par suite, elle admet un plus petit élément. ⊠

Remarques :

- *par convention, on pose $pgcd(0,0) = 0$, et pour tout $a \in \mathbb{Z}$, $ppcm(a,0) = 0$;*
- *par définition, $pgcd(a,b) \in \mathbb{N}^\star$, c'est-à-dire $pgcd(a,b) > 0$. En effet, on a vu que $1 \in D(a,b)$ donc $\max D(a,b) \geqslant 1$;*
- *$\forall a \in \mathbb{Z}$, $pgcd(a,0) = |a|$;*
- *$\forall a,b \in \mathbb{Z}$, $pgcd(a,b) \leqslant \min(|a|,|b|)$ et $ppcm(a,b) \leqslant |a| \times |b|$.*

On admet provisoirement la proposition suivante.

Proposition 5.1.5.2 *Soient $a,b \in \mathbb{Z} \setminus \{-1,0,1\}$. On suppose :*

$$|a| = \prod_{i=1}^{n} p_i^{\alpha_i} \quad \text{et} \quad |b| = \prod_{i=1}^{n} p_i^{\beta_i}$$

où $n \in \mathbb{N}^\star$, les p_i sont premiers et distincts deux à deux, et $\alpha_i, \beta_i \in \mathbb{N}$ (éventuellement nuls). Alors :

$$pgcd(a,b) = \prod_{i=1}^{n} p_i^{\min(\alpha_i,\beta_i)} \quad \text{et} \quad ppcm(a,b) = \prod_{i=1}^{n} p_i^{\max(\alpha_i,\beta_i)}$$

Théorème 5.1.5.3 *Soient $a, b \in \mathbb{Z}$. Alors :*

$$a\mathbb{Z} + b\mathbb{Z} = pgcd(a,b)\mathbb{Z} \quad et \quad a\mathbb{Z} \cap b\mathbb{Z} = ppcm(a,b)\mathbb{Z}$$

Preuve :

• Si $ab = 0$, la propriété est claire. On suppose donc que $a \neq 0$ et $b \neq 0$.

• Montrons que $a\mathbb{Z} \cap b\mathbb{Z} = \text{ppcm}(a,b)\mathbb{Z}$.
Tout d'abord, $a\mathbb{Z}$ et $b\mathbb{Z}$ sont des sous-groupes de $\mathbb{Z}$. Par suite, $a\mathbb{Z} \cap b\mathbb{Z}$ est un sous-groupe de $\mathbb{Z}$ et il existe $n \in \mathbb{N}$ tel que $a\mathbb{Z} \cap b\mathbb{Z} = n\mathbb{Z}$, et nécessairement, $n \neq 0$ (car $|ab| \neq 0$). Montrons que $n = \text{ppcm}(a,b)$.

- ∗ Pour commencer, $n \in a\mathbb{Z}$ donc $a|n$ et de même, $b|n$. Avec les notations précédentes, on a donc montré que $n \in M(a,b) \cap \mathbb{N}^\star$.
- ∗ Par ailleurs, si $p \in M(a,b) \cap \mathbb{N}^\star$, alors $a|p$ et $b|p$. Par suite, $p \in a\mathbb{Z}$ et $p \in b\mathbb{Z}$. Il s'ensuit que : $p \in a\mathbb{Z} \cap b\mathbb{Z} = n\mathbb{Z}$. Par conséquent, $n|p$. Or, $p \in \mathbb{N}^\star$ et $n \in \mathbb{N}$ donc $n|p$ entraîne que $n \leqslant p$.

Ainsi, on a montré que : $\forall p \in M(a,b) \cap \mathbb{N}^\star$, $n \leqslant p$ et $n \in M(a,b) \cap \mathbb{N}^\star$, c'est-à-dire que n est le plus petit élément de $M(a,b) \cap \mathbb{N}^\star$, soit encore $n = \text{ppcm}(a,b)$.

• Montrons à présent que $a\mathbb{Z} + b\mathbb{Z} = \text{pgcd}(a,b)\mathbb{Z}$.
Pour commencer, on montre que $a\mathbb{Z} + b\mathbb{Z} = \{an + bp \ , \ (n,p) \in \mathbb{Z}^2\}$ est un sous-groupe de $\mathbb{Z}$.

- ∗ $0 \in a\mathbb{Z} + b\mathbb{Z}$ puisque $0 = a \times 0 + b \times 0$ et $(0,0) \in \mathbb{Z}^2$;
- ∗ soient $x, y \in a\mathbb{Z} + b\mathbb{Z}$. Par définition, il existe $n, n', p'p' \in \mathbb{Z}$ tels que $x = na + pb$ et $y = n'a + p'b$. Alors, $x - y = (n - n')a + (p - p')b$ et donc $x - y \in a\mathbb{Z} + b\mathbb{Z}$.

Ce qui prouve que $a\mathbb{Z} + b\mathbb{Z}$ est un sous-groupe de $\mathbb{Z}$: il existe donc $d \in \mathbb{N}$ tel que $a\mathbb{Z} + b\mathbb{Z} = d\mathbb{Z}$. Montrons alors que $d = \text{pgcd}(a,b)$.

- ∗ Dans un premier temps, $a \in a\mathbb{Z} + b\mathbb{Z} = d\mathbb{Z}$: par suite, $d|a$. De la même façon, $d|b$. Il s'ensuit que $d \in D(a,b)$.
- ∗ Par ailleurs, soit $p \in D(a,b)$. Par définition, $p|a$ et $p|b$. Il existe donc deux entiers relatifs k et l tels que $a = kp$ et $b = lp$. De plus, $d \in d\mathbb{Z} = a\mathbb{Z} + b\mathbb{Z}$: il existe $(u,v) \in \mathbb{Z}^2$ tels que $ua + vb = d$. En remplaçant, on obtient : $d = (uk + vl)p$, c'est-à-dire $p|d$. Par suite, $p \leqslant |p| \leqslant |d| = d$.

Ce qui montre que $d \in D(a,b)$ et $\forall p \in D(a,b)$, $p \leqslant d$, c'est-à-dire $d = \max D(a,b) = \text{pgcd}(a,b)$.

⊠

En fait, dans la démonstration, on a démontré quelque chose de plus précis sur les diviseurs communs et les multiples communs de deux entiers.

Proposition 5.1.5.4 *Soient $a, b, n \in \mathbb{Z}$. Alors :*

$$\begin{cases} n|a \\ n|b \end{cases} \iff n|pgcd(a,b) \quad et \quad \begin{cases} a|n \\ b|n \end{cases} \iff ppcm(a,b)|n$$

Enfin, la proposition suivante est évidente et sa preuve est laissée en exercice.

Proposition 5.1.5.5 *Soit $(a, b) \in \mathbb{Z}^2$. Alors pour tout $k \in \mathbb{Z}$,*

$$pgcd(ka, kb) = |k| \times pgcd(a,b) \quad et \quad ppcm(ka, kb) = |k| \times ppcm(a,b)$$

Remarque : *en fait, on peut généraliser la notion de pgcd et de ppcm à n entiers ($n \geqslant 2$). Les définitions et les propriétés sont identiques, tout comme les démonstrations.*

5.1.6 Théorème de Bézout et algorithme d'Euclide

On a vu une méthode pour déterminer le pgcd de deux entiers à partir de leur décomposition en facteurs premiers. Seul inconvénient : cela nécessite de connaître la décomposition en facteurs premiers, ce qui n'est pas toujours facile à obtenir.
On dispose d'une autre méthode, appelée algorithme d'Euclide, qui repose sur la remarque suivante et sur le lemme suivant :

Remarque : pour tout $(a, b) \in \mathbb{Z}^2$,

$$\text{pgcd}(a,b) = \text{pgcd}(a,|b|) = \text{pgcd}(|a|,|b|)$$

Lemme 5.1.6.1 *Soient $a, b, q, r \in \mathbb{Z}$ tels que $a = qb + r$. Alors :*

$$pgcd(a,b) = pgcd(b,r)$$

Preuve :

On montre que $D(a,b) = D(b,r)$, ce qui prouvera le lemme.

• Montrons que $D(a,b) \subset D(b,r)$.

Soit $d \in D(a,b)$. Si $d = 0$, alors $a = b = 0$ et donc $r = 0$. Par suite, $d|r$. Sinon, $d|a$ et $d|b$ équivaut à $a \equiv 0\,[d]$ et $b \equiv 0\,[d]$. On en déduit que :

$$r = a - qb \equiv 0 \quad [d] \qquad \text{c'est-à-dire } d|r$$

Par suite, $d|b$ et $d|r$ donc $d \in D(b,r)$.

• Montrons l'inclusion réciproque : $D(b,r) \subset D(a,b)$.

Soit $d \in D(b,r)$. Si $d = 0$, alors $b = r = 0$ et donc $a = 0$. Par suite, $d|a$. Sinon, $b \equiv 0\,[d]$ et $r \equiv 0\,[d]$. Par conséquent, $a \equiv 0\,[d]$, c'est-à-dire $d|a$ et donc $d \in D(a,b)$.

⊠

Théorème 5.1.6.2 (Algorithme d'Euclide) *Soient $a \in \mathbb{Z}$ et $b \in \mathbb{N}^\star$. On pose alors :*

- *$x_0 = a$, $y_0 = b$ et q_0 et r_0 le quotient et le reste de la division euclidienne de a par b ;*
- *si $r_0 = 0$, on s'arrête et sinon, on pose : $x_1 = b$, $y_1 = r_0$ et q_1, r_1 le quotient et le reste de la division euclidienne de x_1 par y_1 ;*
- *puis pour $n \in \mathbb{N}$, si $r_{n+1} = 0$, on s'arrête ; sinon, lorsque $r_{n+1} \neq 0$, on pose $x_{n+2} = r_n$, $y_{n+2} = r_{n+1}$ et on note q_{n+2} et r_{n+2} le quotient et le reste de la division euclidienne de x_{n+2} par y_{n+2}.*

Avec les définitions ci-dessus, il y a deux cas possibles :

1. *soit $r_0 = 0$ et l'algorithme est fini. Dans ce cas, $pgcd(a,b) = b$;*
2. *ou bien $r_0 \neq 0$. Dans ce cas, il existe un entier p tel que $r_p \neq 0$ et $r_{p+1} = 0$. De plus, on a alors :*

$$pgcd(a,b) = r_p$$

Preuve :

Le cas où $r_0 = 0$ est évident.

On suppose donc $r_0 \neq 0$, c'est-à-dire $0 < r_0 < b$. Par définition, pour un entier n donné, si $r_n \neq 0$, alors r_{n+1} est le reste de la division euclidienne de x_{n+1} par $y_{n+1} = r_n$, donc $0 \leqslant r_{n+1} < r_n$.

Si pour tout entier n, $r_n \neq 0$, alors la suite $(r_n)_{n\in\mathbb{N}}$ est une suite strictement décroissante d'entiers compris dans $[\![1, b]\!]$. Ceci est impossible puisque $[\![1, b]\!]$ est un ensemble fini.

Par conséquent, il existe un entier n tel que $r_n = 0$. De plus par hypothèse, $r_0 \neq 0$, donc il existe un entier p tel que $r_{p+1} = 0$. Par définition de l'algorithme, $r_p \neq 0$.
Si $p = 0$, c'est-à-dire $r_1 = 0$, alors $\text{pgcd}(b, r_0) = r_0$ et d'après le lemme précédent :

$$\text{pgcd}(a, b) = \text{pgcd}(b, r_0) = r_0 = r_p$$

De même, si $p = 1$, alors $r_2 = 0$ et :

$$\text{pgcd}(a, b) = \text{pgcd}(b, r_0) = \text{pgcd}(r_0, r_1) = r_1 = r_p$$

Sinon, toujours par application du lemme précédent, on a :

$$\forall k \in [\![1, p-1]\!] \ , \ \text{pgcd}(r_{k-1}, r_k) = \text{pgcd}(r_k, r_{k+1})$$

Par suite,

$$\text{pgcd}(a, b) = \text{pgcd}(b, r_0) = \text{pgcd}(r_0, r_1) = \text{pgcd}(r_{p-1}, r_p) = r_p$$

puisque $r_{p+1} = 0$ signifie que r_p divise r_{p-1}.

⊠

Exemple 5.1.6.3 On détermine le pgcd de 6468 et 1547 par l'algorithme d'Euclide :

$$\begin{array}{rcl} 6468 &=& 4 \times 1547 + 280 \\ 1547 &=& 5 \times 280 + 147 \\ 280 &=& 1 \times 147 + 133 \\ 147 &=& 1 \times 133 + 14 \\ 133 &=& 9 \times 14 + 7 \\ 14 &=& 2 \times 7 + 0 \end{array}$$

Par suite, le dernier reste non nul est $r_4 = 7$ et $\text{pgcd}(6468, 1547) = 7$.

Définition 5.1.6.4 On dit que deux entiers relatifs a et b sont premiers entre eux si $\text{pgcd}(a, b) = 1$.

Exemple 5.1.6.5 2 et 3 sont premiers entre eux, tout comme 24 et 35. En revanche, 21 et 33 ne sont pas premiers entre eux.

Théorème 5.1.6.6 (Bézout) *Soient a et b deux entiers relatifs. Alors :*

$$a \wedge b = 1 \iff \exists (u,v) \in \mathbb{Z}^2 \ , \ au + bv = 1$$

Preuve :

Soit $d = \text{pgcd}(a,b)$. On a déjà vu que $a\mathbb{Z} + b\mathbb{Z} = d\mathbb{Z}$. On a alors :

$$\begin{aligned} \text{pgcd}(a,b) = 1 &\iff a\mathbb{Z} + b\mathbb{Z} = \mathbb{Z} \\ &\iff 1 \in a\mathbb{Z} + b\mathbb{Z} \\ &\iff \exists (u,v) \in \mathbb{Z}^2 \ , \ au + bv = 1 \end{aligned}$$

⊠

Remarque : *l'égalité $au + bv = 1$ est appelée identité de Bézout.*

⚠ **Attention :** ce résultat est très faux si le pgcd n'est pas égal à 1 !!!

$$\exists (u,v) \in \mathbb{Z}^2 \ , \ au + bv = d \iff \text{pgcd}(a,b) | d$$

Il y a alors logiquement deux questions intéressantes que vous devez vous poser !

1. Comment fait-on dans la pratique pour déterminer un couple (u,v) ?
2. Le couple (u,v) est-il unique ?

Pour la seconde question, la réponse est trivialement non ! En effet, si (u_0, v_0) est un couple vérifiant la relation de Bézout, il est clair que pour tout $k \in \mathbb{Z}$, $(u_o - kb, v_0 + ka)$ est aussi un couple vérifiant la relation de Bézout.

Pour la première question, on dispose d'une méthode « simple » pour trouver un couple (u,v). Il est obtenu à partir de l'algorithme d'Euclide. Reprenons l'exemple précédent.

Exemple 5.1.6.7 On a vu que $\text{pgcd}(6468, 1547) = 7$. Reprenons alors les étapes de l'algorithme d'Euclide mais de la fin vers le début.

$$\begin{aligned} 7 &= 133 - 9 \times 14 \\ &= 133 - 9 \times (147 - 1 \times 133) \\ &= 10 \times 133 - 9 \times 147 \\ &= 10 \times (280 - 147) - 9 \times 147 \\ &= 10 \times 280 - 19 \times (1547 - 5 \times 280) \\ &= 105 \times (6468 - 4 \times 1547) - 19 \times 1547 \\ &= 105 \times 6468 - 439 \times 1547 \end{aligned}$$

Remarque : *pour information, une équation de la forme $ax + by = c$ avec $a, b, c \in \mathbb{Z}$, d'inconnues $(x, y) \in \mathbb{Z}^2$ est appelée une équation diophantienne. On sait d'ailleurs résoudre ce type d'équations diophantiennes, c'est-à-dire déterminer toutes les solutions. Une équation diophantienne en général est une équation algébrique, à coefficients entiers, dont on cherche les solutions entières. Par exemple, $y^2 = x^3 + 17$ est une équation diophantienne. La plus connue : $x^n + y^n = z^n$ où n est un entier supérieur ou égal à 3.*
En général, ce sont des problèmes difficiles à résoudre et qui nécessitent des "outils" mathématiques beaucoup plus avancés.

5.1.7 Lemme d'Euclide et théorème de Gauss

Théorème 5.1.7.1 (de Gauss) *Soit $(a, b, c) \in \mathbb{Z}^3$. On a :*

$$\begin{cases} a|bc \\ \\ pgcd(a, b) = 1 \end{cases} \implies a|c$$

Preuve :

On suppose que $a|bc$ et que $a \wedge b = 1$. Par définition, il existe $n \in \mathbb{Z}$ tel que $bc = na$. Par ailleurs, d'après le théorème de Bézout, il existe $(u, v) \in \mathbb{Z}^2$ tel que $au + bv = 1$. On en déduit que :

$$c = c \times 1 = auc + bvc = auc + vna = a(uc + vn)$$

Par suite, $a|c$.

⊠

Corollaire 5.1.7.2 *Soient $(a, c) \in \mathbb{Z}^2$, $n \in \mathbb{N}^\star$ et $(b_1, \cdots, b_n) \in \mathbb{Z}^n$. Alors :*

$$\begin{cases} a| \left(c \times \displaystyle\prod_{i=1}^{n} b_i \right) \\ \\ \forall i \in [\![1, n]\!] \ , \ a \wedge b_i = 1 \end{cases} \implies a|c$$

Preuve :

On montre le résultat par récurrence sur $n \geqslant 1$.

Initialisation :

Pour $n = 1$, c'est le théorème de Gauss que l'on vient de prouver. La propriété est donc vraie au rang 1.

Hérédité :

On suppose la propriété vraie au rang $n \geqslant 1$, c'est-à-dire que pour tout $c \in \mathbb{Z}$ et tout $(b_1, \cdots, b_n) \in \mathbb{Z}^n$ tels que $a|c \times \prod_{i=1}^{n} b_i$ et pour tout $i \in [\![1, n]\!]$, $a \wedge b_i = 1$, $a|c$.
Montrons que la propriété est vraie au rang $n+1$.
Soient $c \in \mathbb{Z}$ et $(b_1, \cdots, b_{n+1}) \in \mathbb{Z}^{n+1}$ tels que a divise $c \times \prod_{i=1}^{n+1} b_i$ et pour tout $i \in [\![1, n+1]\!]$, $a \wedge b_i = 1$. Posons :

$$c' = c \times \prod_{i=1}^{n} b_i$$

Alors, $a|(c' \times b_{n+1})$ et $a \wedge b_{n+1} = 1$. D'après le théorème de Gauss, $a|c'$.
D'après l'hypothèse de récurrence, $a|c$.
Ce qui montre que la propriété est vraie au rang $n+1$ et achève la récurrence.

⊠

Remarque : *on peut aussi démontrer ce corollaire directement en utilisant le lemme d'Euclide (voir juste après) et en remarquant que :*

$$\forall i \in [\![1, n]\!] \ , \ a \wedge b_i = 1 \Longrightarrow a \wedge \left(\prod_{i=1}^{n} b_i \right) = 1$$

Exercice 5.1.7.3 Faire la preuve en utilisant le lemme d'Euclide puis proposer une autre preuve de la remarque utilisant la relation de Bézout.

Corollaire 5.1.7.4 *Soient $a \in \mathbb{Z}$, $n \in \mathbb{N}^\star$ et $(b_1, \cdots, b_n) \in \mathbb{Z}^n$. On suppose que :*

(i) les b_i sont deux à deux premiers entre eux, c'est-à-dire pour tout $(i, j) \in [\![1, n]\!]^2$, $i \neq j \Longrightarrow pgcd(b_i, b_j) = 1$;

(ii) pour tout $i \in [\![1, n]\!]$, $b_i|a$.

Alors $\prod_{i=1}^{n} b_i | a$.

Preuve :

On démontre par récurrence finie que : $\forall k \in [\![1, n]\!]$, $\prod_{i=1}^{k} b_i | a$.

Initialisation :

Par hypothèse, $b_1|a$ donc la propriété est vraie au rang $k = 1$.

Hérédité :

On suppose la propriété vraie au rang $1 \leqslant k < n$. Montrons qu'elle est vraie au rang $k+1$. D'après l'hypothèse de récurrence, $d_k = \prod_{i=1}^{k} b_i$ divise a. Il existe donc $c \in \mathbb{Z}$ tel que :

$$a = c \times \prod_{i=1}^{k} b_i$$

Or, $b_{k+1}|a$, c'est-à-dire $b_{k+1}|cd_k$ et pour tout $i \in [\![1,k]\!]$, $b_{k+1} \wedge b_i = 1$. D'après le corollaire précédent, $b_{k+1}|c$.
Ce qui montre que la propriété est vraie au rang $k+1$ et achève la récurrence.
⊠

Corollaire 5.1.7.5 (Lemme d'Euclide) *Soit p un nombre premier. Alors, pour tout $(a,b) \in \mathbb{Z}^2$:*

$$p|ab \Longrightarrow p|a \ \ ou \ \ p|b$$

Preuve :

Supposons que $p|ab$ et $p \not| a$. Montrons que $p|b$. p étant un nombre premier, les seuls diviseurs de p sont $-1, 1, p$ et $-p$. Par conséquent, si $p \not| a$, alors les seuls diviseurs communs de a et p sont ± 1. Par suite, $a \wedge p = 1$. On a alors $p|ab$ et $a \wedge p = 1$, donc d'après le théorème de Gauss, $p|b$.
⊠

Corollaire 5.1.7.6 *Soient p un nombre premier, $n \in \mathbb{N}$ et $a_0, \cdots, a_n$ des entiers relatifs. Alors :*

$$p \left| \left(\prod_{i=0}^{n} a_i \right) \right. \Longrightarrow \exists i \in [\![0,n]\!] \ , \ p|a_i$$

Exercice 5.1.7.7 Montrer le lemme d'Euclide sans utiliser le théorème de Gauss (on pourra utiliser la relation de Bézout).

Remarque : *on peut traduire le lemme d'Euclide en termes de congruences : si p est un nombre premier, alors :*

$$a \times b \equiv 0 \ \ [p] \ \Longrightarrow (a \equiv 0 \ \ [p] \quad ou \quad b \equiv 0 \ \ [p] \ )$$

Ceci se traduit par une propriété d'intégrité de l'anneau $\mathbb{Z}/p\mathbb{Z}$ que nous n'allons pas étudier. Le lecteur intéressé pourra consulter l'annexe ou tout ouvrage d'algèbre de licence.

On est maintenant en mesure de démontrer l'unicité (à l'ordre près) de la décomposition en facteurs premiers.

Preuve de l'unicité (à l'ordre près) de la décomposition en facteurs premiers :

Montrons par récurrence sur $r \in \mathbb{N}^\star$, la propriété $P(r)$ suivante : pour tous nombres premiers distincts $p_1, \cdots, p_r$ et tous entiers naturels non nuls $\alpha_1, \cdots, \alpha_r$, si

$$\prod_{i=1}^{r} p_i^{\alpha_i} = \prod_{j=1}^{s} q_j^{\beta_j}$$

avec q_j des nombres premiers deux à deux distincts et $\beta_j \in \mathbb{N}^\star$, alors :

— $s = r$;
— il existe une permutation σ de $[\![1, r]\!]$ telle que :

$$\forall i \in [\![1, n]\!] \ , \ q_i = p_{\sigma(i)} \text{ et } \beta_i = \alpha_{\sigma(i)}$$

Initialisation :

Pour $r = 1$, on suppose que $p_1^{\alpha_1} = \prod_{j=1}^{s} q_j^{\beta_j}$ avec p_1 premier, $\alpha_1 \in \mathbb{N}^\star$, $s \in \mathbb{N}^\star$ et où les nombres q_j $(1 \leqslant j \leqslant s)$ sont premiers et deux à deux distincts et $\beta_j \in \mathbb{N}^\star$.

Alors, p_1 divise $a = \prod_{j=1}^{s} q_j^{\beta_j}$. p_1 étant premier, d'après le lemme d'Euclide (ou son corollaire), il existe $j \in [\![1, s]\!]$ tel que $p_1 | q_j$.
Or, q_j est lui aussi premier, donc ses seuls diviseurs sont 1 et lui-même. Par suite, $p_1 = q_j$.

Si $s \neq 1$, soit $i \in [\![1, s]\!]$ tel que $i \neq j$. Alors $q_i | a$ et $a = p_1^{\alpha_1}$ donc $q_i | p_1$ (toujours d'après le lemme d'Euclide). p_1 étant premier, $q_i = p_1 = q_j$, ce qui est absurde (puisqu'on a supposé les q_j deux à deux distincts). Par suite, $s = 1 = r$. On a alors nécessairement $j = 1$ et $p_1^{\alpha_1} = q_1^{\beta_1} = p_1^{\beta_1}$.
Si $\alpha_1 \neq \beta_1$, mettons $\alpha_1 < \beta_1$, alors, $\mathbb{Z}$ étant intègre, $p_1^{\beta_1 - \alpha_1} = 1$. Mais dans ce cas, $\beta_1 - \alpha_1 > 0$ donc p_1 divise 1, ce qui est absurde.
Finalement, $\alpha_1 = \beta_1$ et en prenant $\sigma = \mathrm{Id}_{[\![1,1]\!]}$, la propriété est vraie au rang $r = 1$.

Hérédité :
On suppose la propriété vraie au rang $r \geqslant 1$ et on montre qu'elle est vraie au rang $r + 1$.

Considérons $p_1, \cdots, p_{r+1}$ des nombres premiers distincts, $\alpha_1, \cdots, \alpha_{r+1}$ des entiers naturels non nuls, $s \in \mathbb{N}^\star$, $q_1, \cdots, q_s$ des nombres premiers deux à deux distincts et $\beta_1, \cdots, \beta_s$ des entiers naturels non nuls tels que :

$$(E) : \quad \prod_{i=1}^{r+1} p_i^{\alpha_i} = \prod_{j=1}^{s} q_j^{\beta_j} := a$$

On a alors $p_{r+1} | a$. p_{r+1} étant premier, d'après le lemme d'Euclide, il existe $j \in [\![1, s]\!]$ tel que $p_{r+1} | q_j$. À nouveau, q_j étant lui aussi premier, il vient $p_{r+1} = q_j$.

Si $\alpha_{r+1} < \beta_j$, alors en simplifiant (E) par $p_{r+1}^{\alpha_{r+1}}$ (possible car $\mathbb{Z}$ est intègre), on obtient :

$$\prod_{i=1}^{r} p_i^{\alpha_i} = \prod_{\substack{k=1 \\ k \neq j}}^{s} q_k^{\beta_k} \times p_{r+1}^{\beta_j - \alpha_{r+1}}$$

Dans ce cas, p_{r+1} divise $\prod_{i=1}^{r} p_i^{\alpha_i}$ et p_{r+1} est premier : il existe $i \in [\![1, r]\!]$ tel que $p_{r+1} | p_i$. D'où l'on déduit $p_{r+1} = p_i$ ce qui est absurde.

De la même façon, si $\alpha_{r+1} > \beta_j$, alors $q_j = p_{r+1}$ divise $\prod_{\substack{k=1 \\ k \neq j}}^{s} q_k^{\beta_k}$ donc il existe $i \in [\![1, s]\!] \setminus \{j\}$ tel que $q_j | q_i$. q_i étant premier, $q_i = q_j$ avec $i \neq j$, ce qui est impossible. Par suite, $\alpha_{r+1} = \beta_j$.

Ainsi, on a montré qu'il existe $j \in [\![1, s]\!]$ tel que $q_j = p_{r+1}$ et $\alpha_{r+1} = \beta_j$. Si $s = 1$, on obtient :

$$\prod_{i=1}^{r} p_i^{\alpha_i} = 1$$

Ce qui est impossible puisque $r \geqslant 1$. Par conséquent, $s \geqslant 2$ et on en déduit que :

$$\prod_{i=1}^{r} p_i^{\alpha_i} = \prod_{\substack{k=1 \\ k \neq j}}^{s} q_k^{\beta_k}$$

Considérons l'application :

$$\psi : \begin{array}{ccc} [\![1, s]\!] \setminus \{j\} & \longrightarrow & [\![1, s-1]\!] \\ k & \longmapsto & \begin{cases} k & \text{si } k < j \\ k-1 & \text{si } k > j \end{cases} \end{array}$$

Il est clair que ψ est bijective. On pose alors :

$$\forall i \in [\![1, s-1]\!] \ , \ q'_i = q_{\psi^{-1}(i)} \quad \text{et} \quad \beta'_i = \beta_{\psi^{-1}(i)}$$

Autrement dit, pour $k \in [\![1, s-1]\!]$:

$$q'_k = \begin{cases} q_k & \text{si } 1 \leqslant k < j \\ q_{k+1} & \text{si } j \leqslant k \leqslant s-1 \end{cases}$$

On a alors :

$$\prod_{i=1}^{r} p_i^{\alpha_i} = \prod_{\substack{k=1 \\ k \neq j}}^{s} q_k^{\beta_k} = \prod_{k=1}^{s-1} q_{\psi^{-1}(k)}^{\beta_{\psi^{-1}(k)}} = \prod_{k=1}^{s-1} q_k'^{\beta'_k}$$

Les nombres q'_k sont des nombres premiers deux à deux distincts (puisque ψ^{-1} est injective) et les β'_k sont des entiers naturels non nuls. On peut alors appliquer l'hypothèse de récurrence :

- $s - 1 = r$, c'est-à-dire $s = r + 1$;
- Il existe une permutation σ de $[\![1, r]\!] = [\![1, s-1]\!]$ telle que :

$$\forall i \in [\![1, r]\!] \ , \ q'_i = p_{\sigma(i)} \quad \text{et} \quad \beta'_i = \alpha_{\sigma(i)}$$

Pour finir, on considère l'application suivante :

$$\tau : \begin{array}{ccc} [\![1, r+1]\!] & \longrightarrow & [\![1, r+1]\!] \\ i & \longmapsto & \begin{cases} r+1 & \text{si } i = j \\ \sigma \circ \psi(i) & \text{sinon} \end{cases} \end{array}$$

Il est assez simple de voir que τ est une permutation de $[\![1, r+1]\!]$ car σ et ψ sont des injections et $r + 1 \notin \mathrm{Im}(\sigma \circ \psi)$) et de plus,

$$\forall k \in [\![1, r+1]\!] \setminus \{j\} \ , \ q_k = q'_{\psi(k)} = p_{\sigma(\psi(k))} = p_{\tau(k)}$$

et

$$\forall k \in [\![1, r+1]\!] \ \ \beta_k = \beta'_{\psi(k)} = \alpha_{\sigma(\psi(k))} = \alpha_{\tau(k)}$$

et $q_j = p_{r+1} = p_{\tau(j)}$ et $\beta_j = \alpha_{r+1} = \alpha_{\tau(j)}$.

Ce qui montre que la propriété est vraie au rang $r + 1$ et achève la récurrence.

⊠

Remarque : *on peut aussi maintenant démontrer la proposition 5.1.5.2. Si*

$$|a| = \prod_{i=1}^{n} p_i^{\alpha_i} \quad \textit{et} \quad |b| = \prod_{i=1}^{n} p_i^{\beta_i}$$

On vérifie sans peine que $d = \prod_{i=1}^{n} p_i^{Min(\alpha_i, \beta_i)}$ *est un diviseur commun de a et b. De plus, si N divise a (et b), alors le lemme d'Euclide montre que les diviseurs premiers de N sont parmi les* p_i *et que l'exposant de* p_i *dans la décomposition de N (si* p_i *apparaît dans cette décomposition) est nécessairement inférieur ou égal à* α_i *(et* β_i*), c'est-à-dire inférieur ou égal à* $Min(\alpha_i, \beta_i)$*. Par suite,* $N|d$*.*

5.2 Exercices

Exercice 5.2.1 Quel est le dernier chiffre de l'écriture en base 10 de 7^{7^7} ?

Exercice 5.2.2 Montrer que :

$$\forall n \in \mathbb{Z}\ ,\ 6|\, 5n^3+n\ \ ,\ \ \forall n \in \mathbb{Z}\ ,\ 120|\, n^5-5n^3+4n \quad \text{et} \quad \forall n \in \mathbb{N}\ ,\ n^2|\, (n+1)^n-1$$

Exercice 5.2.3 Soit $n \in \mathbb{N}$ avec $n \geqslant 2$. Démontrer que $\mathcal{P} \cap [\![n!+2, n!+n]\!] = \emptyset$ ($\mathcal{P}$ désigne l'ensemble des nombres premiers).

Exercice 5.2.4 Déterminer tous les entiers n tels que $pgcd(2n+8, 3n+15) = 6$.

Exercice 5.2.5 On divise deux entiers a et b par leur différence $a-b$. Comparer les quotients et les restes obtenus.

Exercice 5.2.6 Déterminer tous les entiers $n \in \mathbb{N}$ tels que $1 \leqslant n \leqslant 105$ sachant que les restes des divisions euclidiennes de n par 3, 5 et 7 sont respectivement 1, 2 et 3.

Exercice 5.2.7 Résoudre dans $\mathbb{Z}^2$ l'équation $9x+15y=18$.

Exercice 5.2.8 Montrer que pour tout entier $n > 1$, $\displaystyle\sum_{k=1}^{n} \frac{1}{k} \notin \mathbb{N}$ (on pourra pour cela considérer l'unique entier $p \geqslant 1$ tel que $2^p \leqslant n < 2^{p+1}$).

Exercice 5.2.9 Soit p un nombre premier.

1. Montrer que pour tout entier k tel que $1 \leqslant k \leqslant p-1$, p divise $\binom{p}{k}$.
2. En déduire que pour tout entier a, $a^p \equiv a \ \ [p]$.
3. En déduire le petit théorème de Fermat : *si p est premier et si a est premier avec p, alors $p|(a^{p-1}-1)$.*

Exercice 5.2.10 Soient a et n deux entiers naturels supérieurs ou égaux à 2.

1. Montrer que si a^n-1 est premier, alors $a=2$ et n est premier. La réciproque est-elle vraie ?
2. Montrer que si a^n+1 est premier, alors a est pair et n est une puissance de 2.

Exercice 5.2.11 Montrer qu'il existe une infinité de nombres premiers dans $4\mathbb{N}+3$.

Exercice 5.2.12 Montrer que l'équation $15x^2-4y^2=3^z$ n'a pas de solution dans $\mathbb{N}^3$.

Exercice 5.2.13 Soit $n \in \mathbb{N}\backslash\{0,1\}$ et $n = \prod_{k=1}^{s} p_k^{\alpha_k}$ sa décomposition en facteurs premiers. Quel est le nombre de diviseurs de n dans $\mathbb{N}^\star$?

Exercice 5.2.14 Montrer qu'il n'existe pas de nombre premier s'écrivant sous la forme $p = \frac{a^3+b^3}{2}$ avec $a, b \in \mathbb{N}$.

Exercice 5.2.15 Soit n un entier dont l'écriture en base 10 est $n = \overline{aabb}$. Déterminer parmi ces entiers n, ceux qui sont des carrés parfaits.

Exercice 5.2.16 Le but de cet exercice est de montrer qu'il existe un multiple de 2012 dont l'écriture décimale ne comporte que des 4.

1. Résultat intermédiaire : le petit théorème de Fermat revisité.

   Soit p un nombre premier et a un entier premier avec p, c'est-à-dire que p ne divise pas a. Pour chaque entier k, on appelle q_k et r_k le quotient et le reste de la division euclidienne de ka par p. On définit alors :

   $$\begin{array}{rccc} f : & [\![1, p-1]\!] & \longrightarrow & [\![1, p-1]\!] \\ & k & \longmapsto & r_k \end{array}$$

   (a) Montrer que f est bien définie et qu'elle est bijective.

   (b) Justifier alors que : $\prod_{k=1}^{p-1}(ka) \equiv \prod_{k=1}^{p-1} f(k) \quad [p]$.

   (c) En déduire que $a^{p-1} \equiv 1 \quad [p]$.
2. Décomposer 2012 en facteurs premiers. On montrera clairement que les facteurs obtenus sont premiers.
3. En vous aidant des deux questions précédentes, montrer que $\underbrace{444....44}_{502\,termes}$ est un multiple de 2012.

Exercice 5.2.17 (Beaucoup plus difficile *)** Soit $f : \mathbb{N}^\star \longrightarrow \mathbb{N}$ une application telle que :

$$\left\{ \begin{array}{l} f(1) = 0 \\ f(p) = 1 \text{ pour tout nombre premier } p \\ \forall n, m \in \mathbb{N}^\star \ , \ f(mn) = mf(n) + f(m)n \end{array} \right.$$

1. Pour tout entier $n \geqslant 2$, exprimer $f(n)$ en utilisant la décomposition en facteurs premiers de n.
2. Résoudre l'équation $f(n) = n$.
3. Montrer que $\forall n \in \mathbb{N}$, $\left(\left\{ \begin{array}{l} 4 < n \\ 4|n \end{array} \right. \implies \left\{ \begin{array}{l} n < f(n) \\ 4|f(n) \end{array} \right. \right)$.
4. En déduire la limite de $f^k(63)$ lorsque k tend vers $+\infty$.

5.3 Annexe

5.3.1 Anneaux $\mathbb{Z}/n\mathbb{Z}$ et quelques propriétés

Définition 5.3.1.1 Soit $n \in \mathbb{N}^\star$. Pour $x \in \mathbb{Z}$, on note $\bar{x} = \{y \in \mathbb{Z} \ / \ y \equiv x \ \ [n] \ \}$, c'est-à-dire $\bar{x} = x + n\mathbb{Z}$ et on définit :

$$\mathbb{Z}/n\mathbb{Z} = \{\bar{x} \ , \ x \in \mathbb{Z}\}$$

Remarques :

- *on retrouve la même notation et les mêmes idées que dans la construction de $\mathbb{Z}$. L'ensemble $\mathbb{Z}/n\mathbb{Z}$ est l'ensemble des classes d'équivalences pour la relation de congruence (modulo n) ;*
- *on vérifie sans peine que pour $(x, y) \in \mathbb{Z}^2$, $\bar{x} = \bar{y} \iff x \equiv y \ \ [n] \iff y \in \bar{x}$.*

Proposition 5.3.1.2 *$\mathbb{Z}/n\mathbb{Z}$ est un ensemble fini et $|\mathbb{Z}/n\mathbb{Z}| = n$.*

Preuve :

Montrons que $\mathbb{Z}/n\mathbb{Z} = \{\bar{0}, \cdots, \overline{n-1}\}$.

Soit $a \in \mathbb{Z}/n\mathbb{Z}$. Par définition, il existe $x \in \mathbb{Z}$ tel que $a = \bar{x}$. Notons alors r le reste de la division euclidienne de x par n. Alors $x \equiv r \ \ [n]$ et d'après la remarque $\bar{x} = \bar{r}$ avec $r \in [\![0, n-1]\!]$. Ce qui prouve l'inclusion $\mathbb{Z}/n\mathbb{Z} \subset \{\bar{0}, \cdots, \overline{n-1}\}$. La réciproque est évidente.

$\boxtimes$

Définition 5.3.1.3 On définit deux lois de composition internes sur $\mathbb{Z}/n\mathbb{Z}$ de la façon suivante : pour $a, b \in \mathbb{Z}/n\mathbb{Z}$, on fixe $x, y \in \mathbb{Z}$ tels que $a = \bar{x}$ et $b = \bar{y}$, on pose alors :

$$a \oplus b = \overline{x + y} \quad \text{et} \quad a \otimes b = \overline{x \times y}$$

Proposition 5.3.1.4 *Les lois de compositions internes $\oplus$ et $\otimes$ sur $\mathbb{Z}/n\mathbb{Z}$ sont bien définies.*

Preuve :

C'est une conséquence directe de la compatibilité de $\equiv$ avec l'addition et la multiplication. En effet, il s'agit de prouver que la définition posée ne dépend pas du choix « du représentant ». Autrement dit, si on choisit $x, x', y, y' \in \mathbb{Z}$ tels que $a = \bar{x} = \bar{x'}$ et $b = \bar{y} = \bar{y'}$, on veut montrer que :

$$\overline{x+y} = \overline{x'+y'} \quad \text{et} \quad \overline{x \times y} = \overline{x' \times y'}$$

mais ceci est équivalent à dire que si $x \equiv x' \ [n]$ et $y \equiv y' \ [n]$, alors :

$$x + y \equiv x' + y' \ [n] \quad \text{et} \quad x \times y \equiv x' \times y' \ [n]$$

Cette propriété a déjà été vue (proposition 5.1.1.4).

$\boxtimes$

Théorème 5.3.1.5 $(\mathbb{Z}/n\mathbb{Z}, \oplus, \otimes)$ *est un anneau commutatif et l'application :*

$$\pi : \begin{array}{ccc} \mathbb{Z} & \longrightarrow & \mathbb{Z}/n\mathbb{Z} \\ x & \longmapsto & \bar{x} \end{array}$$

est un morphisme surjectif d'anneaux dont le noyau est $n\mathbb{Z}$. L'application π est appelée la surjection canonique.

Preuve :

On remarque que, par définition des opérations $\oplus$ et $\otimes$, on a :

$$\forall (x, y) \in \mathbb{Z}^2 \ , \ \pi(x+y) = \pi(x) \oplus \pi(y) \ \text{ et } \ \pi(x \times y) = \pi(x) \otimes \pi(y)$$

De la structure d'anneau commutatif pour $(\mathbb{Z}, +, \times)$, on déduit facilement que $(\mathbb{Z}/n\mathbb{Z}, \oplus, \otimes)$ est un anneau commutatif dont l'élément neutre est $\pi(1_{\mathbb{Z}})$, ce qui permet avec les deux égalités ci-dessus de conclure que π est bien un morphisme d'anneaux.
Enfin, $\ker(\pi) = \{x \in \mathbb{Z} \ / \ \pi(x) = \pi(0)\} = \{x \in \mathbb{Z} \ / \ x \equiv 0 \, [n] \}$, c'est-à-dire $\ker(\pi) = n\mathbb{Z}$.

$\boxtimes$

Remarque : *vous pouvez toujours faire toutes les vérifications « à la main » pour vérifier que $(\mathbb{Z}/n\mathbb{Z}, \oplus, \otimes)$ est un anneau commutatif si les arguments présentés dans la preuve sont trop rapides.*

5.3.2 Corps $\mathbb{Z}/p\mathbb{Z}$ et éléments inversibles de $\mathbb{Z}/n\mathbb{Z}$

Théorème 5.3.2.1 *Soit $n \geqslant 2$ un entier. Alors sont équivalents :*

(i) $\mathbb{Z}/n\mathbb{Z}$ est un corps ;

(ii) $\mathbb{Z}/n\mathbb{Z}$ est un anneau intègre ;

(iii) n est premier.

Lorsque $n = p$ est premier, le corps $\mathbb{Z}/p\mathbb{Z}$ est noté $\mathbb{F}_p$: c'est un corps fini à p éléments.

Preuve :

On sait qu'un anneau fini est intègre si et seulement si c'est un corps (voir exercice 1.3.16). Par ailleurs,

- si n est premier, alors le lemme d'Euclide montre que $\overline{x} \otimes \overline{y} = \overline{0}$ implique que $\overline{x} = \overline{0}$ ou $\overline{y} = \overline{0}$ donc $\mathbb{Z}/n\mathbb{Z}$ est intègre ;
- et si n est composé, alors $n = ab$ avec $1 < a < n$ et $1 < b < n$ et par suite $\overline{a} \otimes \overline{b} = \overline{0}$ avec $\overline{a} \neq \overline{0}$ et $\overline{b} \neq \overline{0}$. Ce qui montre que $\mathbb{Z}/n\mathbb{Z}$ n'est pas intègre. ⊠

Proposition 5.3.2.2 *Soit $n \geqslant 2$ un entier et soit $x \in \mathbb{Z}$. Alors les énoncés suivants sont équivalents :*

(i) $\overline{x}$ est inversible dans $\mathbb{Z}/n\mathbb{Z}$;

(ii) $x \wedge n = 1$.

Preuve :

• Montrons $(i) \Longrightarrow (ii)$.
On suppose que $\overline{x}$ est inversible dans l'anneau $(\mathbb{Z}/n\mathbb{Z}, \oplus, \otimes)$. Alors il existe $y \in \mathbb{Z}$ tel que $\overline{x} \otimes \overline{y} = \overline{1}$, c'est-à-dire $\overline{x \times y} = \overline{1}$ (par définition de $\otimes$). Par conséquent, $x \times y - 1 \in n\mathbb{Z}$ et il existe $u \in \mathbb{Z}$ tel que $xy - 1 = un$. On en déduit donc que $yx + (-u)n = 1$ et donc d'après le théorème de Bézout, $x \wedge n = 1$.

• Réciproquement, si $x \wedge n = 1$, il existe $(u, v) \in \mathbb{Z}^2$ tel que $ux + vn = 1$. Mais alors :

$$1_{\mathbb{Z}/n\mathbb{Z}} = \overline{1} = \overline{ux + vn} = (\overline{u} \otimes \overline{x}) \oplus (\overline{v} \otimes \overline{n}) = \overline{u} \otimes \overline{x}$$

Ce qui prouve qu'il existe $\overline{u} \in \mathbb{Z}/n\mathbb{Z}$ tel que $\overline{u} \otimes \overline{x} = 1_{\mathbb{Z}/n\mathbb{Z}}$. $\mathbb{Z}/n\mathbb{Z}$ étant commutatif, on a donc prouvé que $\overline{x}$ est inversible. ⊠

Chapitre 6

Fonctions réelles ou complexes d'une variable réelle

Prérequis : dans tout ce chapitre, les notions suivantes sont supposées connues :

- structures usuelles : groupes, anneaux et corps ; morphismes de groupes ou d'anneaux ;
- structure d'espace vectoriel, sous-espace vectoriel et application linéaire ;
- relation d'équivalence, relation d'ordre, borne inférieure et borne supérieure ;
- ensemble $\mathbb{R}$, borne supérieure dans $\mathbb{R}$ et sa caractérisation ;
- suites réelles : convergence, divergence, théorème de Bolzano-Weierstrass ;
- nombres complexes : module, partie réelle et partie imaginaire ;
- propriétés « informelles » sur les fonctions de classe $\mathcal{C}^n$;
- propriétés « informelles » des o, O et équivalents ;
- propriétés de base sur l'intégration (pour certains exemples).

Aucune connaissance spécifique sur la continuité ou la notion de limite n'est supposée connue.

6.1 Généralités sur les fonctions d'une variable réelle

Dans tout ce chapitre, I désigne un intervalle réel non vide et non réduit à un point, $\mathbb{K}$ désigne soit $\mathbb{R}$, soit $\mathbb{C}$. Lorsque $\mathbb{K}$ est utilisé, cela veut dire que la définition ou la propriété est valable dans les deux cas (c'est-à-dire cas réel et cas complexe).

Essentiellement, toutes les définitions ou propriétés qui utilisent la relation d'ordre dans $\mathbb{R}$ ne peuvent pas s'étendre à $\mathbb{C}$ (comme pour les suites).

6.1.1 Ensemble $\mathcal{F}(I,\mathbb{K})$ et relation d'ordre

On a déjà vu dans le chapitre sur les suites (voir proposition 3.1.2.3) que :

Proposition 6.1.1.1 *L'ensemble $\mathcal{F}(I,\mathbb{K})$ est muni de deux lois de composition interne, une loi de composition externe, définies pour tous $f,g\in\mathcal{F}(I,\mathbb{K})$ et tout $\lambda\in\mathbb{K}$ par :*

$$\begin{array}{rcl} f+g\,:\,I & \longrightarrow & \mathbb{K} \\ x & \longmapsto & f(x)+g(x) \end{array} \quad ; \quad \begin{array}{rcl} f\times g\,:\,I & \longrightarrow & \mathbb{K} \\ x & \longmapsto & f(x)\times g(x) \end{array} \quad ; \quad \begin{array}{rcl} \lambda\cdot f\,:\,I & \longrightarrow & \mathbb{K} \\ x & \longmapsto & \lambda f(x) \end{array}$$

Alors $(\mathcal{F}(I,\mathbb{K}),+,\times)$ est un anneau commutatif et $(\mathcal{F}(I,\mathbb{K}),+,\cdot)$ est un $\mathbb{K}$-espace vectoriel.

De plus, si $\mathbb{K}=\mathbb{R}$, on munit $\mathcal{F}(I,\mathbb{R})$ de la relation : $f\leqslant g \iff \forall x\in I\ ,\ f(x)\leqslant g(x)$. Alors $(\mathcal{F}(I,\mathbb{R}),\leqslant)$ est partiellement ordonné.

Définition 6.1.1.2 Soient $f,g\in\mathcal{F}(I,\mathbb{R})$. On définit alors les fonctions :

$$\begin{array}{rcl} \sup(f,g)\,:\,I & \longrightarrow & \mathbb{R} \\ x & \longmapsto & \max(f(x),g(x)) \end{array} \quad ; \quad \begin{array}{rcl} \inf(f,g)\,:\,I & \longrightarrow & \mathbb{R} \\ x & \longmapsto & \min(f(x),g(x)) \end{array}$$

et

$$\begin{array}{rcl} |f|\,:\,I & \longrightarrow & \mathbb{R} \\ x & \longmapsto & |f(x)| \end{array}$$

Remarque : *en particulier, on a donc $|f|=\sup(-f,f)$.*

Exercice 6.1.1.3 Soient f et g définies sur $\mathbb{R}$ par : $\forall x\in\mathbb{R}\ ,\ f(x)=x$ et $g(x)=2-x$. Représenter graphiquement f, g, $\sup(f,g)$ et $\inf(f,g)$.

Remarque : *$\sup(f,g)$ a la propriété de la borne supérieure dans $\mathcal{F}(I,\mathbb{R})$, c'est-à-dire que $\sup(f,g)$ est le plus petit des majorants de l'ensemble $\{f,g\}$.*

Remarque : *il peut aussi être utile de définir la partie positive et la partie négative d'une fonction f :*

$$f_+ = \sup(f, 0) \quad ; \quad f_- = \sup(-f, 0) \quad ; \quad f = f_+ - f_- \quad et \quad |f| = f_+ + f_-$$

On remarque que f_+ (la partie positive de f) et f_- (la partie négative de f) sont des fonctions positives.

6.1.2 Ensemble $\mathcal{B}(I, \mathbb{K})$

Définition 6.1.2.1 On dit qu'une application $f : I \longrightarrow \mathbb{R}$ est :

- majorée s'il existe $M \in \mathbb{R}$ tel que $f \leqslant M$, *i.e.* $\exists M \in \mathbb{R}$, $\forall x \in I$, $f(x) \leqslant M$;
- minorée s'il existe $m \in \mathbb{R}$ tel que $m \leqslant f$, *i.e.* $\exists m \in \mathbb{R}$, $\forall x \in I$, $m \leqslant f(x)$;
- bornée (sur I) si elle est majorée et minorée.

On dit qu'une fonction $f : I \longrightarrow \mathbb{C}$ est bornée si : $\exists M \geqslant 0$, $\forall x \in I$, $|f(x)| \leqslant M$.

Remarque : *comme pour les suites, on a une seconde caractérisation des fonctions bornées. En effet, f est bornée sur I si et seulement si $|f|$ est majorée sur I. On retrouve d'ailleurs la définition du cas des fonctions à valeurs complexes.*

Exemple 6.1.2.2 Les fonctions cos, sin, arctan et th sont bornées sur $\mathbb{R}$. Argch est minorée mais non majorée sur $[1, +\infty[$ et Argsh n'est ni majorée, ni minorée sur $\mathbb{R}$.

Proposition 6.1.2.3 *L'ensemble $\mathcal{B}(I, \mathbb{K})$ des applications bornées sur I est une sous-algèbre de $\mathcal{F}(I, \mathbb{K})$, c'est-à-dire un sous-espace vectoriel et un sous-anneau.*

Preuve :

La démonstration est identique à celle déjà vue dans le cadre des suites. On rappelle que pour montrer que c'est une sous-algèbre, on doit vérifier (ou montrer) que :

- $\mathcal{B}(I, \mathbb{K}) \subset \mathcal{F}(I, \mathbb{K})$;
- $1_{\mathcal{F}(I,\mathbb{K})} \in \mathcal{B}(I, \mathbb{K})$;
- $\forall (f, g) \in \mathcal{B}(I, \mathbb{K})^2$, $\forall (\lambda, \mu) \in \mathbb{K}^2$, $\lambda \cdot f + \mu \cdot g \in \mathcal{B}(I, \mathbb{K})$;
- $\forall (f, g) \in \mathcal{B}(I, \mathbb{K})^2$, $f \times g \in \mathcal{B}(I, \mathbb{K})$.

$\boxtimes$

Remarque : concrètement, la proposition précédente signifie que les combinaisons linéaires et les produits de fonctions bornées sont encore des fonctions bornées.

Définition 6.1.2.4 Soit $f \in \mathcal{F}(I, \mathbb{R})$. On définit alors (sous réserve d'existence) :

$$\max_I f = \max_{x \in I} f(x) = \max(f(I)) \qquad \text{et} \qquad \min_I f = \min_{x \in I} f(x) = \min(f(I))$$

$$\sup_I f = \sup_{x \in I} f(x) = \sup(f(I)) \qquad \text{et} \qquad \inf_I f = \inf_{x \in I} f(x) = \inf(f(I))$$

Étant entendu que $\max f$ et $\min f$ n'existent pas toujours. En revanche, on peut toujours définir $\sup f$ et $\inf f$ dans $\overline{\mathbb{R}}$.

Exemple 6.1.2.5 Soit $f : x \longmapsto \dfrac{1}{1+x^2}$. Alors $\max_{\mathbb{R}} f = 1$, $\sup_{\mathbb{R}} f = \max f$, $\min_{\mathbb{R}} f$ n'est pas défini mais $\inf_{\mathbb{R}} f = 0$.

⚠ **Attention :** on ne doit jamais écrire $\max_I f$ et $\min_I f$ sans avoir justifié l'existence ! De même, en toute rigueur, il faudrait préciser si on parle de borne supérieure dans $\mathbb{R}$ ou dans $\overline{\mathbb{R}}$. Pour éviter cette confusion (et les erreurs graves qui s'ensuivent), on ne considère que des bornes supérieure ou inférieure dans $\mathbb{R}$ et il faut alors justifier l'existence.

Exercice 6.1.2.6 Déterminer, s'ils existent, $\max_{\mathbb{R}} \mathrm{th}$, $\min_{\mathbb{R}} \mathrm{th}$, $\sup_{\mathbb{R}} \mathrm{th}$, $\inf_{\mathbb{R}} \mathrm{th}$.

Définition 6.1.2.7 Soit $f : I \longrightarrow \mathbb{R}$ une fonction. On dit que :

- f admet un maximum en a si $\max_{x \in I} f(x) = f(a)$;
- f admet un minimum en a si $\min_{x \in I} f(x) = f(a)$;
- f admet un extremum en a si f admet un maximum en a ou bien un minimum en a.

Remarque : *si f admet un maximum sur I, ce maximum est unique ! C'est par définition* $\max\{f(x)\ ,\ x \in I\}$. *En revanche, le ou les points où f atteint son maximum ne sont pas forcément uniques ! Par exemple, la fonction cosinus admet un maximum sur $\mathbb{R}$ qui vaut 1 et ce maximum est atteint en chaque point $x_n = 2n\pi$, avec $n \in \mathbb{Z}$.*

Proposition 6.1.2.8 *Par définition, on a pour toute* $f \in \mathcal{F}(I, \mathbb{R})$ *:*

$$f \text{ majorée sur } I \iff \sup_I f \in \mathbb{R} \quad ; \quad f \text{ minorée sur } I \iff \inf_I f \in \mathbb{R}$$

En particulier, f *est bornée sur* I *si et seulement si* $\sup_I f$ *et* $\inf_I f$ *sont finis (c'est-à-dire sont des réels).*

Preuve :

C'est évident car par exemple $\sup_I f = \sup\{f(x)\ ,\ x \in I\}$. Or, l'ensemble $A = \{f(x)\ ,\ x \in I\} = f(I)$ est une partie non vide de $\mathbb{R}$. Elle admet donc une borne supérieure (dans $\mathbb{R}$) si et seulement si elle est majorée. ⊠

Remarque : *dans la pratique, on montre que* f *est majorée sur* I *pour justifier l'existence de* $\sup_I f$ *(autrement dit, on ne considère que des bornes supérieures dans* $\mathbb{R}$*).*

6.1.3 Fonctions périodiques

Définition 6.1.3.1 On dit qu'une application $f : I \longrightarrow \mathbb{K}$ est périodique s'il existe un réel $T > 0$ tel que :

(i) $\forall x \in I\ ,\ (x + T) \in I$;

(ii) $\forall x \in I\ ,\ f(x + T) = f(x)$.

Un tel nombre réel T est alors appelé une période de f et on dit que f est une fonction T-périodique (ou une fonction périodique de période T).

Exemple 6.1.3.2 Soit $T > 0$. Alors pour tout $n \in \mathbb{N}$, les fonctions c_n et s_n définies sur $\mathbb{R}$ par :

$$\forall x \in \mathbb{R}\ ,\ c_n(x) = \cos\left(\frac{2n\pi}{T}x\right) \quad \text{et} \quad s_n(x) = \sin\left(\frac{2n\pi}{T}x\right)$$

sont des fonctions T-périodiques.

Remarque : *sur ce dernier exemple, on voit bien qu'une fonction peut admettre plusieurs périodes. C'est pour cela qu'on dit bien que* T *est une période de la fonction.*

Exercice 6.1.3.3 Déterminer toutes les périodes (positives) de $f = \chi_{\mathbb{Q}}$ (la fonction caractéristique de $\mathbb{Q}$).

Proposition 6.1.3.4 *Soit $T > 0$. L'ensemble des fonctions T-périodiques est un sous-espace vectoriel et un sous-anneau de $\mathcal{F}(I, \mathbb{K})$. Autrement dit, c'est une sous-algèbre de $\mathcal{F}(I, \mathbb{K})$.*
Par ailleurs, on peut limiter l'étude d'une fonction T-périodique à un intervalle de longueur T.

Preuve :

• Pour montrer que l'ensemble des fonctions T-périodiques est une sous-algèbre de $\mathcal{F}(I, \mathbb{K})$, on doit montrer que :

(i) la fonction constante sur I, égale à 1, est T-périodique (c'est évident) ;

(ii) si f, g sont deux fonctions T-périodiques et λ, μ sont deux nombres dans $\mathbb{K}$, alors :

∗ $f \times g$ est T-périodique (à nouveau, c'est évident) ;

∗ $\lambda \cdot f + \mu \cdot g$ est T-périodique (encore évident).

• Enfin, il est clair que la connaissance de f sur un intervalle de longueur T est suffisante. ⊠

Remarques :

- *bien entendu, il ne faut pas oublier qu'une fonction périodique n'est pas nécessairement définie sur $\mathbb{R}$ tout entier, comme par exemple la fonction* tan *;*
- *pour plus de détails sur l'ensemble des périodes d'une fonction périodique, voir l'exercice 2.4.8.3 (question 5(d)).*

6.1.4 Fonctions paires et fonctions impaires

Définition 6.1.4.1 On dit qu'une fonction $f : I \longrightarrow \mathbb{K}$ est :

- paire si : $\forall x \in I$, $(-x) \in I$ et $\forall x \in I$, $f(-x) = f(x)$;
- impaire si : $\forall x \in I$, $(-x) \in I$ et $\forall x \in I$, $f(-x) = -f(x)$.

Rappel : *si $\mathbb{K} = \mathbb{R}$, c'est-à-dire si f est à valeurs réelles, alors, en notant $\mathcal{C}_f$ la courbe représentative de f dans un repère orthonormé, on a :*

$$f \text{ est paire} \iff \mathcal{C}_f \text{ est symétrique par rapport à l'axe des ordonnées}$$
$$f \text{ est impaire} \iff \mathcal{C}_f \text{ est symétrique par rapport à l'origine}$$

Proposition 6.1.4.2 *On suppose que I est symétrique par rapport à 0. Soit $\mathcal{P}$ (respectivement $\mathcal{I}$) l'ensemble des fonctions paires (respectivement impaires). Alors :*

(i) *$\mathcal{P}$ est une sous-algèbre de $\mathcal{F}(I,\mathbb{K})$;*

(ii) *$\mathcal{I}$ est un sous-espace vectoriel de $\mathcal{F}(I,\mathbb{K})$ mais n'est pas un sous-anneau ;*

(iii) *$\mathcal{P}$ et $\mathcal{I}$ sont des sous-espaces vectoriels supplémentaires dans $\mathcal{F}(I,\mathbb{K})$, c'est-à-dire $\mathcal{P}\oplus\mathcal{I}=\mathcal{F}(I,\mathbb{K})$.*

Autrement dit, toute fonction $f : I \longrightarrow \mathbb{K}$ se décompose de façon unique sous la forme $f = p + i$, avec p une fonction paire et i une fonction impaire. On dit que p est la partie paire de f et i est la partie impaire de f. Par ailleurs, p et i sont alors données par :

$$\forall x \in I\ ,\ p(x) = \frac{f(x)+f(-x)}{2} \quad et \quad \forall x \in I\ ,\ i(x) = \frac{f(x)-f(-x)}{2}$$

Preuve :

• Montrons (i), c'est-à-dire que :

  ∗ la fonction constante sur I égale à 1 est paire (évident) ;

  ∗ $\forall f,g \in \mathcal{P}\ ,\ \forall \lambda,\mu \in \mathbb{K}\ ,\ f\times g \in \mathcal{P}$ et $(\lambda\cdot f+\mu\cdot g)\in\mathcal{P}$ (clair).

• Montrons (ii), c'est-à-dire que :

  — la fonction nulle appartient à $\mathcal{I}$ (clair) ;

  — $\forall f,g \in \mathcal{I}\ ,\ \forall \lambda,\mu \in \mathbb{K}\ ,\ \lambda\cdot f+\mu\cdot g \in \mathcal{I}$ (encore clair).

Par ailleurs, il est clair que la fonction constante égale à 1 n'est pas une fonction impaire donc $\mathcal{I}$ n'est pas un sous-anneau de $\mathcal{F}(I,\mathbb{K})$.

• On a déjà prouvé (iii) deux fois : une fois dans le cours de logique (exemple de raisonnement par analyse-synthèse) et une fois dans le cours sur les espaces vectoriels (en utilisant les propriétés des symétries).

⊠

Exemple 6.1.4.3 Soit $f : x \longmapsto e^{ix}$. Alors la partie paire de f est $x \longmapsto \cos(x)$ et la partie impaire de f est $x \longmapsto i\sin(x)$ (attention, la partie impaire n'est donc pas la partie imaginaire car il y a bien le terme i en plus).

Exercice 6.1.4.4 Retrouver directement que $\mathcal{I}$ et $\mathcal{P}$ sont des sous-espaces vectoriels à l'aide d'une application linéaire.

Exercice 6.1.4.5 Quelles sont les parties paire et impaire de la fonction $x \longmapsto e^x$?

Remarques :

- *on peut vérifier que le produit de deux fonctions impaires est une fonction paire ;*
- *l'expression des parties paire et impaire d'une fonction f permet directement de montrer que f est de classe $\mathcal{C}^n$ si et seulement si ses parties paire et impaire le sont.*

6.1.5 Fonctions lipschitziennes

Définition 6.1.5.1 Soit $f : I \longrightarrow \mathbb{K}$ une application.

- Soit $k \in \mathbb{R}^+$. On dit que f est k-lipschitzienne si :

$$\forall (x, y) \in I^2 \ , \ |f(y) - f(x)| \leqslant k|y - x|$$

- On dit que f est lipschitzienne s'il existe $k \geqslant 0$ tel que f soit k-lipschitzienne.
- Si f est k-lipschitzienne avec $0 \leqslant k < 1$, on dit que f est k-contractante.

Exercice 6.1.5.2 Montrer que les fonctions affines sont lipschitziennes sur $\mathbb{R}$.

Exemple 6.1.5.3 Les fonctions sinus et cosinus sont 1-lipschitziennes. En effet, soient x et y deux réels, alors :

$$\begin{aligned}
|\cos(y) - \cos(x)| &= \left| \int_x^y \cos'(t)\,\mathrm{d}t \right| \\
&= \left| \int_x^y -\sin(t)\,\mathrm{d}t \right| \\
&\leqslant \int_I |\sin(t)|\,\mathrm{d}t \quad (\text{où } I = [x, y] \text{ si } x \leqslant y \text{ et } I = [y, x] \text{ sinon}) \\
&\leqslant \int_I \mathrm{d}t \\
&\leqslant |y - x|
\end{aligned}$$

Remarque : *pour le moment, retenez bien cette technique pour montrer qu'une fonction de classe $\mathcal{C}^1$ est lipschitzienne. On verra dans le cours de mathématiques supérieures 2 que lorsque f est dérivable sur I, f est lipschitzienne sur I si et seulement si f' est bornée sur I.*

Exemple 6.1.5.4 La fonction $x \longmapsto x^2$ n'est pas lipschitzienne sur $\mathbb{R}$. Par contre, elle l'est sur tout segment.

En effet, raisonnons par l'absurde et supposons que la fonction carré soit lipschitzienne sur $\mathbb{R}$. Alors, il existe $k \geqslant 0$ tel que : $\forall x, y \in \mathbb{R}$, $|y^2 - x^2| \leqslant k|y - x|$. En particulier, en prenant $x = 0$, on obtient que : $\forall y \in \mathbb{R}$, $y^2 \leqslant k|y|$. En prenant par exemple $y = k + 1$, on obtient $k \leqslant -1$, ce qui est absurde.

En revanche, sur $I = [a, b]$ avec $a \leqslant b$ deux réels, on a :

$$\forall x, y \in [a, b] \ , \ |y^2 - x^2| = |y + x| \times |y - x| \leqslant \underbrace{(2 \times \max(|a|, |b|))}_{k} |y - x|$$

Exercice 6.1.5.5 Montrer que th est lipschitzienne sur $\mathbb{R}$.

Exercice 6.1.5.6 $x \longmapsto \sqrt{x}$ est-elle lipschitzienne sur $[0, +\infty[$? Sur $]0, +\infty[$? Sur $[a, +\infty[$ (avec $a > 0$) ?

Proposition 6.1.5.7 *Soit $Lip(I, \mathbb{K})$ l'ensemble des applications de I dans $\mathbb{K}$ qui sont lipschitziennes. Alors $Lip(I, \mathbb{K})$ est un sous-espace vectoriel de $\mathcal{F}(I, \mathbb{K})$.*

Preuve :

• Tout d'abord, il est clair que $Lip(I, \mathbb{K}) \subset \mathcal{F}(I, \mathbb{K})$ et que la fonction nulle est lipschitzienne (on a vu que toute fonction affine est lipschitzienne).

• Montrons à présent que $Lip(I, \mathbb{K})$ est stable par combinaisons linéaires. Soient $f, g \in Lip(I, \mathbb{K})$ et $\lambda, \mu \in \mathbb{K}$. $f \in Lip(I, \mathbb{K})$ donc il existe $k \geqslant 0$ tel que f soit k-lipschitzienne. De même, il existe $k' \geqslant 0$ tel que g soit k'-lipschitzienne. Notons $h = \lambda \cdot f + \mu \cdot g$.
On a alors, pour tout $(x, y) \in I^2$:

$$\begin{aligned} |h(y) - h(x)| &= |\lambda \times (f(y) - f(x)) + \mu \times (g(y) - g(x))| \\ &\leqslant |\lambda| \times |f(y) - f(x)| + |\mu| \times |g(y) - g(x)| \\ &\leqslant |\lambda| \times k|y - x| + |\mu| \times k'|y - x| \\ &\leqslant (|\lambda|k + |\mu|k') |y - x| \end{aligned}$$

En posant $K = |\lambda|k + |\mu|k'$, on a bien $K \geq 0$ et $h = \lambda \cdot f + \mu \cdot g$ est K-lipschitzienne. Ainsi, $\lambda \cdot f + \mu \cdot g \in Lip(I, \mathbb{K})$. ⊠

⚠ **Attention :** le produit de deux fonctions lipschitziennes n'est pas toujours une fonction lipschitzienne. Quel contre-exemple pouvez-vous donner à partir des exemples qu'on vient de voir ?

6.1.6 Fonctions monotones

Définition 6.1.6.1 Soit $f : I \longrightarrow \mathbb{R}$ une application. On dit que :

- f est croissante sur I (respectivement strictement croissante sur I) si :

  $\forall x, y \in I\ ,\ x \leqslant y \Longrightarrow f(x) \leqslant f(y)$ (resp. $\forall x, y \in I\ ,\ x < y \Longrightarrow f(x) < f(y)$)

- f est décroissante sur I (respectivement strictement décroissante sur I) si :

  $\forall x, y \in I\ ,\ x \leqslant y \Longrightarrow f(x) \geqslant f(y)$ (resp. $\forall x, y \in I\ ,\ x < y \Longrightarrow f(x) > f(y)$)

- f est monotone sur I (respectivement strictement monotone sur I) si elle est croissante sur I ou décroissante sur I (respectivement strictement croissante sur I ou strictement décroissante sur I).

Remarque : *dans la pratique, pour étudier les variations d'une fonction f, f sera dérivable sur I et on appliquera les méthodes étudiées avant (étude du signe de f') et qui seront démontrées dans le cours de mathématiques supérieures 2.*

Proposition 6.1.6.2 *Soient $f : I \longrightarrow \mathbb{R}$ et $g : J \longrightarrow \mathbb{R}$ deux applications. On suppose que :*

(i) f et g sont monotones sur I et J respectivement ;

(ii) on peut définir la composée $g \circ f$, c'est-à-dire $f(I) \subset J$.

Alors la fonction $g \circ f$ est monotone sur I, la monotonie étant donné par « la règle des signes » (croissante : + , décroissante : -). Autrement dit, si f et g sont de même monotonie, alors $g \circ f$ est croissante et si f et g sont de monotonies opposées, alors $g \circ f$ est décroissante.

Par ailleurs, si f et g sont strictement monotones, alors $g \circ f$ l'est aussi.

Preuve :

Traitons par exemple le cas où f est décroissante sur I et g croissante sur J.
Soient x et y deux éléments de I tels que $x \leqslant y$. Alors $f(y) \leqslant f(x)$ car f est décroissante et puisque g est croissante sur J (et $f(x) \in J$ et $f(y) \in J$), $g(f(y)) \leqslant g(f(x))$, c'est-à-dire $(g \circ f)(y) \leqslant (g \circ f)(x)$.

$\boxtimes$

6.2 Étude locale d'une fonction

Cadre : dans toute la suite, on se restreint à des fonctions définies sur un intervalle réel I ayant au moins deux points, c'est-à-dire tel que $-\infty \leqslant \inf I < \sup I \leqslant +\infty$. Il s'agit donc d'applications de I dans $\mathbb{K}$.

On définit alors :

- l'intérieur de I, noté $\overset{\circ}{I}$, par $\overset{\circ}{I} =]\inf I, \sup I[$ (on a donc dans notre cadre $\underline{\overset{\circ}{I} \neq \emptyset}$) ;
- l'adhérence de I, notée $\overline{I}$, par $\overline{I} = [\inf I, \sup I] \subset \overline{\mathbb{R}}$.

6.2.1 Voisinage d'un point

Définition 6.2.1.1 Soit $a \in \mathbb{R}$. On définit :

- la boule ouverte (respectivement fermée) de centre a et de rayon $\alpha > 0$ par

$$\begin{array}{rrcl} & B(a,\alpha) & = & \{x \in \mathbb{R}\ ,\ |x-a| < \alpha\} \quad = \quad]a-\alpha, a+\alpha[\\ (\textit{respectivement} & B_f(a,\alpha) & = & \{x \in \mathbb{R}\ ,\ |x-a| \leqslant \alpha\} \quad = \quad [a-\alpha, a+\alpha]) \end{array}$$

  Les ensembles $B(a,\alpha)$ pour $\alpha > 0$ sont appelés des voisinages ouverts de a (dans $\mathbb{R}$) et les ensembles $B_f(a,\alpha)$ pour $\alpha > 0$ sont appelés des voisinages fermés de a ;

- un voisinage ouvert (respectivement fermé) de $+\infty$ est un intervalle de la forme $]A, +\infty[$ (respectivement $[A, +\infty[$) avec $A \in \mathbb{R}$;
- un voisinage ouvert (respectivement fermé) de $-\infty$ est un intervalle de la forme $]-\infty, A[$ (respectivement $]-\infty, A]$) avec $A \in \mathbb{R}$.

Notation pour ce cours : on note $\mathcal{V}_f(a)$ l'ensemble des voisinages fermés de a.

Exercice 6.2.1.2 Vérifier que : $a \in \overline{I} \iff \forall V \in V_f(a)\ ,\ I \cap V \neq \emptyset$.

Définition 6.2.1.3 Soit $f : I \longrightarrow \mathbb{K}$ et $a \in \overline{I}$. On dit qu'une propriété relative à f est vraie au voisinage de a (ou localement en a) s'il existe un voisinage ouvert B de a telle que la propriété est vraie sur $I \cap B$.

Remarque : *on peut prouver que l'on obtient une définition équivalente en remplaçant* ***ouvert*** *par* ***fermé*** *dans la définition précédente.*

Exemple 6.2.1.4 La propriété : « f ne s'annule pas au voisinage de 1 » signifie

$$\exists \alpha > 0 \ , \ \forall x \in I \cap]1-\alpha, 1+\alpha[\ , \ f(x) \neq 0$$

ou de façon équivalente, $\exists \alpha > 0 \ , \ \forall x \in I \cap [1-\alpha, 1+\alpha] \ , \ f(x) \neq 0$.

Exemple 6.2.1.5 f est bornée au voisinage de $+\infty$ signifie qu'il existe $A \in \mathbb{R}$ tel que f est bornée sur $[A, +\infty[$.

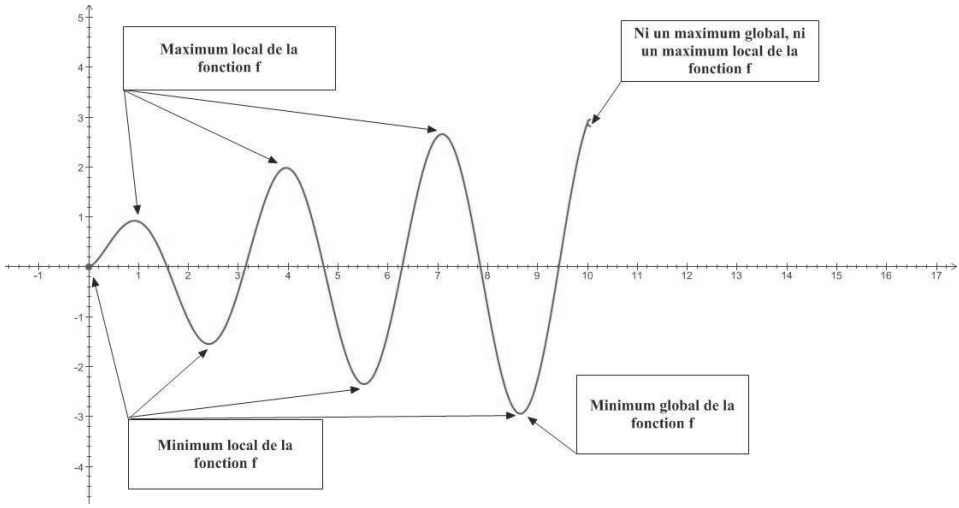
Exemple 6.2.1.6 Soit $f : I \longrightarrow \mathbb{R}$ et soit $a \in I$. f est croissante au voisinage de a si :

$$\exists \alpha > 0 \ , \ \forall x, y \in I \cap]a-\alpha, a+\alpha[\ , \ (x < y \Longrightarrow f(x) \leqslant f(y))$$

Définition 6.2.1.7 Soit $f : I \longrightarrow \mathbb{R}$ une fonction et $a \in I$. On dit que :

- f admet un maximum local en a s'il existe $\alpha > 0$ tel que $f_{|I \cap]a-\alpha, a+\alpha[}$ admet un maximum en a ;
- f admet un minimum local en a s'il existe $\alpha > 0$ tel que $f(a)$ est un minimum de f sur $]a-\alpha, a+\alpha[\cap I$;
- f admet un extremum local en a si f admet un maximum local ou un minimum local en a.

Exemple 6.2.1.8 On donne la courbe représentative suivante :


Maximum local de la fonction f
Ni un maximum global, ni un maximum local de la fonction f
Minimum global de la fonction f
Minimum local de la fonction f

6.2.2 Limite d'une fonction en un point et continuité en un point

Définition 6.2.2.1 Soient $a \in \overline{I}$, $\ell \in \overline{\mathbb{R}}$ et $f : I \longrightarrow \mathbb{R}$. On dit que f admet ℓ pour limite en a si :

$$\forall U \in \mathcal{V}_f(\ell) \ , \ \exists V \in \mathcal{V}_f(a) \ , \ \forall x \in I \cap V \ , \ f(x) \in U$$

On peut néanmoins reformuler ceci de façon plus explicite :

(i) Lorsque $a, \ell \in \mathbb{R}$, f admet ℓ pour limite en a si :

$$\forall \varepsilon > 0 \ , \ \exists \alpha > 0 \ , \ \forall x \in I \ , \ (\ |x - a| \leqslant \alpha \Longrightarrow |f(x) - \ell| \leqslant \varepsilon \ )$$

(ii) Lorsque $a \in \mathbb{R}$ et $\ell = +\infty$, f admet $+\infty$ pour limite en a si :

$$\forall A \in \mathbb{R} \ , \ \exists \alpha > 0 \ , \ \forall x \in I \ , \ (\ |x - a| \leqslant \alpha \Longrightarrow f(x) \geqslant A \ )$$

(iii) Lorsque $a \in \mathbb{R}$ et $\ell = -\infty$, f admet $-\infty$ pour limite en a si :

$$\forall A \in \mathbb{R} \ , \ \exists \alpha > 0 \ , \ \forall x \in I \ , \ (\ |x - a| \leqslant \alpha \Longrightarrow f(x) \leqslant A \ )$$

(iv) Lorsque $a = +\infty$ et $\ell \in \mathbb{R}$, f admet ℓ pour limite en $+\infty$ si :

$$\forall \varepsilon > 0 \ , \ \exists A \in \mathbb{R} \ , \ \forall x \in I \ , \ (\ x \geqslant A \Longrightarrow |f(x) - \ell| \leqslant \varepsilon \ )$$

(v) Lorsque $a = -\infty$ et $\ell \in \mathbb{R}$, f admet ℓ pour limite en $-\infty$ si :

$$\forall \varepsilon > 0 \ , \ \exists A \in \mathbb{R} \ , \ \forall x \in I \ , \ (\ x \leqslant A \Longrightarrow |f(x) - \ell| \leqslant \varepsilon \ )$$

(vi) Lorsque $a = +\infty$ et $\ell = -\infty$, f admet $-\infty$ pour limite en $+\infty$ si :

$$\forall A \in \mathbb{R} \ , \ \exists B \in \mathbb{R} \ , \ \forall x \in I \ , \ (\ x \geqslant B \Longrightarrow f(x) \leqslant A \ )$$

(vii) Lorsque $a = +\infty$ et $\ell = +\infty$, f admet $+\infty$ pour limite en $+\infty$ si :

$$\forall A \in \mathbb{R} \ , \ \exists B \in \mathbb{R} \ , \ \forall x \in I \ , \ (\ x \geqslant B \Longrightarrow f(x) \geqslant A \ )$$

(viii) Lorsque $a = -\infty$ et $\ell = -\infty$, f admet $-\infty$ pour limite en $-\infty$ si :

$$\forall A \in \mathbb{R} \ , \ \exists B \in \mathbb{R} \ , \ \forall x \in I \ , \ (\ x \leqslant B \Longrightarrow f(x) \leqslant A \ )$$

(ix) Lorsque $a = -\infty$ et $\ell = +\infty$, f admet $+\infty$ pour limite en $-\infty$ si :

$$\forall A \in \mathbb{R} \ , \ \exists B \in \mathbb{R} \ , \ \forall x \in I \ , \ (\ x \leqslant B \Longrightarrow f(x) \geqslant A \ )$$

Remarques :

- *vous devez savoir écrire explicitement les définitions de la limite dans les différents cas ($a \in \mathbb{R}$, $a = +\infty$, $a = -\infty$ et de même pour ℓ). La définition avec les voisinages a l'avantage d'être unique (on ne traite pas les différents cas) et de pouvoir se généraliser aux espaces vectoriels normés (cours de mathématiques spéciales 1) ;*
- *de façon équivalente, f admet $\ell \in \mathbb{R}$ pour limite en $a \in \mathbb{R}$ si :*

$$\forall \varepsilon > 0 \ , \ \exists \alpha > 0 \ , \ \forall x \in I \cap [a-\alpha, a+\alpha] \ , \ |f(x) - l| \leqslant \varepsilon$$

Dans la pratique, c'est plutôt cette forme que l'on utilisera (et de même pour les autres cas).

Définition 6.2.2.2 Soient $f : I \longrightarrow \mathbb{C}$, $a \in \overline{I}$ et $\ell \in \mathbb{C}$. On dit que f admet ℓ pour limite en a si :

$$\forall \varepsilon > 0 \ , \ \exists V \in \mathcal{V}_f(a) \ , \ \forall x \in I \cap V \ , \ |f(x) - \ell| \leqslant \varepsilon$$

Remarque : *la définition de la limite pour une fonction à valeurs complexes est donc identique à celle pour les fonctions à valeurs réelles à deux petites différences près :*

(i) lorsque f est à valeurs complexes, $|f(x) - \ell|$ désigne le module (et non la valeur absolue) ;

(ii) il n'y a pas de sens à parler de limite infinie lorsque f est à valeurs complexes.

Par ailleurs, on peut également définir la boule ouverte (respectivement fermée) de centre ℓ et de rayon $\varepsilon > 0$ dans $\mathbb{C}$ de la façon suivante :

$$B(\ell, \varepsilon) = \{z \in \mathbb{C} \ / \ |z - \ell| < \varepsilon\} \ \text{ et } \ B_f(\ell, \varepsilon) = \{z \in \mathbb{C} \ / \ |z - \ell| \leqslant \varepsilon\}$$

En général, dans $\mathbb{C}$, on note plutôt $B(\ell, \varepsilon) = D(\ell, \varepsilon)$ et on parle de disque ouvert (ou fermé) mais ce n'est qu'une notation et du vocabulaire (c'est le même ensemble).

Lemme 6.2.2.3 *Soient $\ell \in \overline{\mathbb{R}}$ et $\ell' \in \overline{\mathbb{R}}$ (ou bien $(\ell, \ell') \in \mathbb{C}^2$). On suppose que $\ell \neq \ell'$. Alors il existe $U \in \mathcal{V}_f(\ell)$ et $V \in \mathcal{V}_f(\ell')$ tels que $U \cap V = \emptyset$.*

Preuve :

Si $(\ell, \ell') \in \mathbb{C}^2$ (contient le cas où ce sont des réels), alors il suffit de choisir $\alpha = \frac{|\ell' - \ell|}{3}$, $U = B_f(\ell, \alpha)$ et $V = B_f(\ell', \alpha)$. Les autres cas sont laissés en exercice.

⊠

Théorème 6.2.2.4 *Soient $a \in \overline{I}$, $\ell \in \overline{\mathbb{R}}$ et $f : I \longrightarrow \mathbb{R}$.*

Si f admet ℓ pour limite en a, alors le nombre ℓ est unique et est noté $\ell = \lim\limits_{x \to a} f(x)$.
De plus, lorsque $\ell \in \mathbb{R}$, on dit que f admet une limite finie au point a.

Preuve :

On raisonne par l'absurde : supposons que f admette deux limites différentes ℓ et ℓ' en a, avec $\ell, \ell' \in \overline{\mathbb{R}}$. Par définition, on a alors :

$$\forall U \in \mathcal{V}_f(\ell)\ ,\ \exists V \in \mathcal{V}_f(a)\ ,\ \forall x \in I \cap V\ ,\ f(x) \in U$$

$$\forall U' \in \mathcal{V}_f(\ell')\ ,\ \exists V' \in \mathcal{V}_f(a)\ ,\ \forall x \in I \cap V'\ ,\ f(x) \in U'$$

Par hypothèse, $\ell \neq \ell'$ donc d'après le lemme précédent, il existe un voisinage fermé U de ℓ et un voisinage fermé U' de ℓ' tels que $U \cap U' = \emptyset$.

On applique alors la définition de la limite pour ces choix de voisinages : il existe un voisinage fermé V de a tel que, pour tout $x \in I \cap V$, $f(x) \in U$. De même, il existe un voisinage fermé V' de a tel que, pour tout $x \in I \cap V'$, $f(x) \in U'$.
Mais alors $V \cap V'$ est aussi un voisinage fermé de a et par définition, $I \cap V \cap V' \neq \emptyset$. Soit alors $x_0 \in I \cap V \cap V'$. Pour un tel x_0, on a $x_0 \in I \cap V$ donc $f(x_0) \in U$ et de même, $x_0 \in I \cap V'$ donc $f(x_0) \in U'$.
Par conséquent, $f(x_0) \in U \cap U'$, ce qui contredit $U \cap U' = \emptyset$. ⊠

Exercice 6.2.2.5 Simplement pour manipuler les définitions explicites, montrer à partir des définitions avec les « ε » et « A » que :

1. Si f admet deux limites finies en $a \in \mathbb{R}$, alors elles sont égales.
2. Si f admet $+\infty$ pour limite en $-\infty$, alors f ne peut pas admettre $\ell \in \mathbb{R}$ pour limite en $-\infty$.
3. Si f admet $-\infty$ pour limite en $+\infty$, alors f ne peut pas admettre $+\infty$ pour limite en $+\infty$.

Théorème 6.2.2.6 *Soient $a \in \overline{I}$, $\ell \in \mathbb{C}$ et $f : I \longrightarrow \mathbb{C}$.*

Si f admet ℓ pour limite en a, alors le nombre ℓ est unique et est noté $\ell = \lim\limits_{x \to a} f(x)$.

Preuve :

Identique au cas réel. ⊠

Exemple 6.2.2.7 Montrons à l'aide de la définition formelle que $\lim_{x\to-\infty} x^2 = +\infty$.
Posons pour $x \in \mathbb{R}$, $f(x) = x^2$. On veut donc montrer que :

$$\forall A \in \mathbb{R}\ ,\ \exists B \in \mathbb{R}\ ,\ \forall x \leqslant B\ ,\ f(x) \geqslant A$$

Soit $A \in \mathbb{R}$. Posons $B = -\sqrt{|A|}$. Alors, la fonction f étant décroissante sur $]-\infty, 0]$, pour tout $x \leqslant B \leqslant 0$, $f(x) \geqslant B^2$, c'est-à-dire $f(x) \geqslant |A| \geqslant A$.
Ainsi, on a montré que : $\lim_{x\to-\infty} f(x) = +\infty$.

Exemple 6.2.2.8 Soit $g(x) = \dfrac{1}{x}$ pour $x > 0$. Montrons que $\lim_{x\to 0} g(x) = +\infty$, c'est-à-dire :

$$\forall A \in \mathbb{R}\ ,\ \exists \alpha > 0\ ,\ \forall x \in [-\alpha, \alpha] \cap]0, +\infty[\ ,\ g(x) \geqslant A$$

Soit $A \in \mathbb{R}^{+\star}$. Posons $\alpha = \dfrac{1}{A}$. Il est alors clair que :

$$\forall x \in]0, \alpha]\ ,\ g(x) \geqslant A$$

D'où le résultat.

Remarque : *j'espère que vous avez remarqué que dans l'exemple précédent, on s'est contenté de prouver le résultat pour $A > 0$. Pourquoi ceci suffit-il ?*

Exemple 6.2.2.9 Montrons que $\lim_{x\to 1} \ln(x) = 0$, c'est-à-dire :

$$\forall \varepsilon > 0\ ,\ \exists \alpha > 0\ ,\ \forall x \in]0, +\infty[\cap [1-\alpha, 1+\alpha]\ ,\ |\ln(x)| \leqslant \varepsilon$$

Soit $\varepsilon > 0$. On cherche $\alpha > 0$ (et $\alpha < 1$ de sorte que $[1-\alpha, 1+\alpha] \subset]0, +\infty[$) tel que :

$$1 - \alpha \leqslant x \leqslant 1 - \alpha \Longrightarrow -\varepsilon \leqslant \ln(x) \leqslant \varepsilon$$

soit encore, tel que :

$$1 - \alpha \leqslant x \leqslant 1 - \alpha \Longrightarrow e^{-\varepsilon} \leqslant x \leqslant e^{\varepsilon}$$

Pour que cette implication soit vraie, il suffit que $e^{-\varepsilon} \leqslant 1 - \alpha$ et $1 + \alpha \leqslant e^{\varepsilon}$, c'est-à-dire il suffit que :

$$0 < \alpha \leqslant 1 - e^{-\varepsilon} \quad \text{et} \quad 0 < \alpha \leqslant e^{\varepsilon} - 1$$

On pose alors $\alpha = \min(\frac{1}{2}, 1 - e^{-\varepsilon}, e^{\varepsilon} - 1)$. Par construction, $\alpha > 0$ (puisque $e^{\varepsilon} - 1 > 0$ et $1 - e^{-\varepsilon} > 0$), $\alpha < 1$ et :

$$\forall x \in [1-\alpha, 1+\alpha]\ ,\ |\ln(x)| \leqslant \varepsilon$$

Ce qui montre que $\lim_{x\to 1} \ln(x) = 0$.

Remarque : *on constate que même des « résultats simples » sur les limites peuvent devenir techniques à établir. C'est pour cela que dans la pratique, on utilise directement les limites de référence !*

Exemple 6.2.2.10 Montrons que $\lim_{x\to 0} e^{ix} = 1$.
Soit $\varepsilon > 0$. On cherche à nouveau $\alpha > 0$ tel que : $|x| \leqslant \alpha \Longrightarrow |e^{ix} - 1| \leqslant \varepsilon$. Or, pour tout réel x,

$$|e^{ix} - 1| = |e^{\frac{ix}{2}}| \times |e^{\frac{ix}{2}} - e^{-\frac{ix}{2}}| = 1 \times |2i\sin(\frac{x}{2})| = 2|\sin(\frac{x}{2})| \leqslant |x|$$

Par suite, si on choisit $\alpha = \varepsilon > 0$, on a bien :

$$\forall x \in [-\alpha, \alpha]\ ,\ |e^{ix} - 1| \leqslant \varepsilon$$

De même que pour les suites (ou les courbes paramétrées), on a la caractérisation suivante qui permet de se ramener à des fonctions réelles.

Proposition 6.2.2.11 *Soient $f : I \longrightarrow \mathbb{C}$ et $a \in \overline{I}$. Alors :*

$$f \text{ a une limite en } a \iff \Re e(f) \text{ et } \Im m(f) \text{ ont des limites } \underline{\text{finies}} \text{ en } a$$

Dans ce cas, $\lim_{x\to a} f(x) = \lim_{x\to a} \Re e(f(x)) + i \lim_{x\to a} \Im m(f(x))$.

Preuve :

Cette propriété découle directement du fait que pour tous nombres complexes z et ℓ,

$$|\Re e(z) - \Re e(\ell)| \leqslant |z - \ell| \leqslant |\Re e(z) - \Re e(\ell)| + |\Im m(z) - \Im m(\ell)|$$

et de même pour la partie imaginaire. On fait néanmoins la preuve pour manipuler les définitions et on fait la preuve dans le cas $a \in \mathbb{R}$.

• On suppose que f admet $\ell \in \mathbb{C}$ pour limite en a. Montrons que $\lim_{x\to a} \Re e(f(x)) = \Re e(\ell)$ et $\lim_{x\to a} \Im m(f(x)) = \Im m(\ell)$,
Soit $\varepsilon > 0$. Puisque $\lim_{x\to a} f(x) = \ell$, il existe $\alpha > 0$ tel que :

$$\forall x \in I \cap [a - \alpha, a + \alpha]\ ,\ |f(x) - \ell| \leqslant \varepsilon$$

On a alors d'après l'inégalité rappelée ci-dessus,

$$\forall x \in I \cap [a - \alpha, a + \alpha]\ ,\ |\Re e(f(x)) - \Re e(\ell)| \leqslant |f(x) - \ell| \leqslant \varepsilon$$

et de même pour la partie imaginaire. Ceci prouve que $\Re e(f)$ admet une limite finie (qui est $\Re e(\ell)$) et $\Im m(f)$ admet une limite finie (qui est $\Im m(\ell)$).

• Réciproquement, on suppose que $\Re e(f)$ admet une limite finie ℓ_1 en a et que $\Im m(f)$ admet une limite finie ℓ_2 en a. Montrons que f admet une limite en a et que $\lim\limits_{x\to a} f(x) = \ell_1 + i\ell_2$.
Soit $\varepsilon > 0$. Par définition de la limite (appliquée avec $\frac{\varepsilon}{2} > 0$), il existe $\alpha_1 > 0$ et $\alpha_2 > 0$ tels que :

$$\forall x \in I \cap [a-\alpha_1, a+\alpha_1] \ , \ |\Re e(f(x)) - \ell_1| \leqslant \frac{\varepsilon}{2}$$

et

$$\forall x \in I \cap [a-\alpha_2, a+\alpha_2] \ , \ |\Im m(f(x)) - \ell_2| \leqslant \frac{\varepsilon}{2}$$

Posons $\alpha = \min(\alpha_1, \alpha_2)$. Alors $\alpha > 0$ et par construction, pour tout $x \in I \cap [a-\alpha, a+\alpha]$:

$$\begin{aligned} |f(x) - (\ell_1 + i\ell_2)| &\leqslant |\Re e(f(x)) - \ell_1| + |\Im m(f(x)) - \ell_2| \\ &\leqslant \frac{\varepsilon}{2} + \frac{\varepsilon}{2} \\ &\leqslant \varepsilon \end{aligned}$$

Ce qui prouve que $\lim\limits_{x\to a} f(x) = \ell_1 + i\ell_2$.

⊠

Remarques :

- *on a donné la preuve dans le cas $a \in \mathbb{R}$ pour éviter l'utilisation des voisinages qui peut parfois paraître trop « abstraite ». Essayez de faire la preuve avec des voisinages, ce qui permet d'éviter de devoir distinguer trois cas : $a \in \mathbb{R}$, $a = +\infty$ et $a = -\infty$;*
- *on verra que cette proposition découle aussi des opérations algébriques sur les limites. En effet, si f admet ℓ pour limite en a, alors $\bar{f}$ admet $\bar{\ell}$ pour limite en a et donc $\Re e(f) = \frac{1}{2}f + \frac{1}{2}\bar{f}$ admet aussi une limite qui est $\frac{1}{2}\ell + \frac{1}{2}\bar{\ell} = \Re e(\ell)$ (et de même pour la partie imaginaire).*

Proposition 6.2.2.12 *Soient $f : I \longrightarrow \mathbb{K}$, $a \in \overline{I}$ et $\ell \in \mathbb{K}$ (ou $\ell \in \overline{\mathbb{R}}$ si $\mathbb{K} = \mathbb{R}$). On a les propriétés suivantes :*

- *lorsque $\ell \in \mathbb{K}$, $\lim\limits_{x\to a} f(x) = \ell \iff \lim\limits_{x\to a} (f(x) - \ell) = 0$;*
- *lorsque $a \in \mathbb{R}$, $\lim\limits_{x\to a} f(x) = \ell \iff \lim\limits_{h\to 0} f(a+h) = \ell$.*

Preuve :

C'est évident et les détails sont laissés en exercice. ⊠

Définition 6.2.2.13 Soit $a \in I$. On dit que f est continue en a si $\lim\limits_{x \to a} f(x)$ existe.

⚠ **Attention :** n'oubliez jamais que pour une fonction à valeurs réelles, l'existence de la limite signifie qu'elle admet une limite finie ou infinie !

Proposition 6.2.2.14 *Soient $f : I \longrightarrow \mathbb{K}$ et $a \in I$. Alors :*

$$f \text{ est continue en } a \iff \lim_{x \to a} f(x) = f(a)$$

Preuve :

• L'implication $\Longleftarrow$ est évidente.

• Réciproquement, on suppose que f est continue en a, c'est-à-dire que f admet une limite en a.

∗ Tout d'abord, on montre que si $\mathbb{K} = \mathbb{R}$ alors la limite de f en a est nécessairement finie (si $\mathbb{K} = \mathbb{C}$ c'est automatiquement vrai par définition de la limite pour une fonction à valeurs complexes).
On raisonne par l'absurde et on suppose dans un premier temps que $\lim\limits_{x \to a} f(x) = +\infty$. On pose $A = f(a) + 1$. Il existe V un voisinage fermé de a tel que :

$$\forall x \in I \cap V \ , \ f(x) \geqslant A$$

Or, $a \in I \cap V$ donc $f(a) \geqslant f(a) + 1$, ce qui est absurde. On montre de la même façon (ou bien en remplaçant f par $-f$ mais les opérations algébriques sur les limites n'ont pas encore été traitées) qu'on ne peut pas avoir $\lim\limits_{x \to a} f(x) = -\infty$.

∗ Ainsi, il existe $\ell \in \mathbb{K}$ tel que $\lim\limits_{x \to a} f(x) = \ell$.
Montrons alors que $\ell = f(a)$. Soit $\varepsilon > 0$. Puisque $a \in I$, $a \in \mathbb{R}$ et par définition de la limite d'une fonction en un point réel, il existe un réel $\alpha > 0$ tel que :

$$\forall x \in I \cap [a - \alpha, a + \alpha] \ , \ |f(x) - \ell| \leqslant \varepsilon$$

Or, $a \in I$ donc $a \in I \cap [a - \alpha, a + \alpha]$. Par suite, $|f(a) - \ell| \leqslant \varepsilon$.
Ainsi, on a prouvé que : $\forall \varepsilon > 0 \ , \ |f(a) - \ell| \leqslant \varepsilon$, d'où $f(a) = \ell$.

⊠

⚠ **Attention :** il n'y a absolument aucun sens à dire que « f est continue en $+\infty$ » ! La notion de continuité est définie pour un point $a \in I$, c'est-à-dire dans l'ensemble de définition de la fonction : $+\infty$ n'appartient jamais à l'ensemble de définition !

Définition 6.2.2.15 Soient $f : I \longrightarrow \mathbb{K}$ et $a \in \overline{I} \cap \mathbb{R}$.

- Si $a \neq \sup I$, on définit la limite de f à droite en a par :

$$\lim_{x \to a^+} f(x) = \lim_{\substack{x \to a \\ x > a}} f(x) = \lim_{x \to a} f_{|I \cap]a, +\infty[}(x)$$

  (à condition que cette limite existe) ;

- Si $a \neq \inf I$, on définit la limite de f à gauche en a par :

$$\lim_{x \to a^-} f(x) = \lim_{\substack{x \to a \\ x < a}} f(x) = \lim_{x \to a} f_{|I \cap]-\infty, a[}(x)$$

  (à condition que cette limite existe) ;

Si $a \in I$, on dit que f est continue à droite (respectivement à gauche) en a si

$$\lim_{\substack{x \to a \\ x > a}} f(x) = f(a) \quad \text{(respectivement } \lim_{\substack{x \to a \\ x < a}} f(x) = f(a)\text{)}$$

Proposition 6.2.2.16 *Soient $f : I \longrightarrow \mathbb{K}$ et $a \in \overset{\circ}{I}$. Alors f est continue en a si et seulement si* $\lim\limits_{\substack{x \to a \\ x > a}} f(x) = \lim\limits_{\substack{x \to a \\ x < a}} f(x) = f(a)$.

Preuve :

• Montrons $\Longrightarrow$

On suppose f continue en a. Soit $\varepsilon > 0$. Il existe $\alpha > 0$ tel que, pour tout $x \in I \cap [a - \alpha, a + \alpha]$, $|f(x) - f(a)| \leqslant \varepsilon$. Il est alors clair que :

$$\forall x \in (I \cap]a, +\infty[) \cap [a - \alpha, a + \alpha] \ , \ |f(x) - f(a)| \leqslant \varepsilon$$

c'est-à-dire $\lim\limits_{\substack{x \to a \\ x > a}} f(x) = f(a)$. On montre de même que $\lim\limits_{\substack{x \to a \\ x < a}} f(x) = f(a)$.

• Montrons $\Longleftarrow$

On suppose que $\lim\limits_{\substack{x \to a \\ x > a}} f(x) = \lim\limits_{\substack{x \to a \\ x < a}} f(x) = f(a)$.

Soit $\varepsilon > 0$. Par définition de la limite à droite et à gauche, il existe $\alpha_1 > 0$ et $\alpha_2 > 0$ tels que :

$$\forall x \in I \cap]a, a+\alpha_1] \ , \ |f(x) - f(a)| \leqslant \varepsilon$$

et

$$\forall x \in I \cap [a-\alpha_2, a[\ , \ |f(x) - f(a)| \leqslant \varepsilon$$

Posons $\alpha = \min\{\alpha_1, \alpha_2\}$. Alors $\alpha > 0$ et pour tout $x \in I \cap [a-\alpha, a+\alpha]$:

$*$ si $x < a$, alors $x \in I \cap [a-\alpha, a[\subset I \cap [a-\alpha_2, a[$ donc $|f(x)-f(a)| \leqslant \varepsilon$;

$*$ si $x = a$, alors $|f(x) - f(a)| = 0 \leqslant \varepsilon$;

$*$ si $x > a$, alors $x \in I \cap]a, a+\alpha] \subset I \cap]a, a+\alpha_1]$ donc $|f(x) - f(a)| \leqslant \varepsilon$.

Ainsi, on a démontré que :

$$\forall \varepsilon > 0 \ , \ \exists \alpha > 0 \ , \ \forall x \in I \cap [a-\alpha, a+\alpha] \ , \ |f(x) - f(a)| \leqslant \varepsilon$$

Ce qui prouve que $\lim\limits_{x \to a} f(x) = f(a)$.

⊠

On retrouve beaucoup de résultats similaires au cas des suites. Seule petite différence, les propriétés que l'on retrouve sont valables localement, c'est-à-dire au voisinage du point où on calcule la limite. On peut citer les deux propriétés importantes suivantes.

Proposition 6.2.2.17 *Soient $f : I \longrightarrow \mathbb{K}$ et $a \in \overline{I}$. Si la fonction f admet une limite finie en a, alors f est bornée au voisinage de a.*

Preuve :

On suppose que $\ell = \lim\limits_{x \to a} f(x)$ existe et $\ell \in \mathbb{K}$ (c'est-à-dire que la limite est finie si $\mathbb{K} = \mathbb{R}$). On pose $\varepsilon = 1 > 0$. Par définition de la limite, il existe un voisinage V de a tel que :

$$\forall x \in I \cap V \ , \ |f(x) - \ell| \leqslant 1$$

Alors, $\forall x \in I \cap V \ , \ |f(x)| \leqslant |\ell| + 1$, avec V un voisinage de a. Ce qui prouve que f est bornée au voisinage de a.

⊠

⚠ **Attention :** tout comme pour les suites, la réciproque est fausse !! f bornée au voisinage de a n'implique pas que f admet une limite finie en a ! Par exemple, la fonction sinus est bornée au voisinage de $+\infty$ mais elle n'admet pas de limite (on montrera cela un peu plus loin lorsqu'on aura fait la caractérisation de la limite par les suites).

Proposition 6.2.2.18 *Soient $f : I \longrightarrow \mathbb{R}$ et $a \in \overline{I}$. On suppose que $\lim_{x\to a} f(x) = \ell$ et que $\ell > 0$. Alors f est minorée par un réel strictement positif au voisinage de a.*

Preuve :

On fait la preuve dans le cas $a = -\infty$.
• On suppose dans un premier temps que $\ell \in \mathbb{R}^{+\star}$. Posons $\varepsilon = \frac{\ell}{2} > 0$. Pour cet $\varepsilon > 0$, il existe $B \in \mathbb{R}$ tel que :

$$\forall x \in I \cap]-\infty, B] \ , \ |f(x) - \ell| \leqslant \varepsilon$$

Alors, pour tout $x \in I \cap]-\infty, B]$:

$$f(x) \geqslant \ell - \varepsilon \text{ c'est-à-dire } \quad f(x) \geqslant \frac{\ell}{2} > 0$$

Ce qui prouve que f est minorée par $\frac{\ell}{2} > 0$ au voisinage de $-\infty$.

• Si $\ell = +\infty$, on applique la définition de la limite avec $A = 1$ (par exemple) et on obtient que $f \geqslant 1$ sur un voisinage de $-\infty$. ⊠

Remarque : *à nouveau l'utilisation des voisinages permet d'éviter de traiter plusieurs cas mais comme mentionné à plusieurs reprises, il est tout aussi important de savoir écrire explicitement les voisinages et c'est un peu moins abstrait qu'avec des voisinages. C'est pour cette raison que les preuves proposées alternent l'utilisation de voisinages et de description explicite dans les cas $a \in \mathbb{R}$, $a = +\infty$ et $a = -\infty$. Le lecteur non satisfait pourra faire toutes les preuves avec des voisinages.*

Exercice 6.2.2.19 Soient $f : \mathbb{R} \longrightarrow \mathbb{Z}$.

1. On suppose que f admet une limite finie en $+\infty$. Montrer que f est constante au voisinage de $+\infty$.
2. Le résultat précédent est-il encore valable si f admet une limite infinie en $+\infty$?

Exercice 6.2.2.20 Donner un exemple de fonction non majorée au voisinage de $+\infty$ mais qui n'admet pas de limite en $+\infty$.

Exercice 6.2.2.21 Soient $f : I \longrightarrow \mathbb{C}$ et $a \in \overline{I}$. On suppose que f admet une limite non nulle en a. Montrer qu'il existe un voisinage de a sur lequel l'application f ne s'annule pas.

Exercice 6.2.2.22 Montrer que la fonction E (partie entière) est continue à droite en tout point de $\mathbb{R}$ et qu'elle admet en tout point une limite finie à gauche.

6.2.3 Opérations algébriques sur les limites

Proposition 6.2.3.1 *Soient $a \in \overline{I}$, A l'ensemble des applications de I dans $\mathbb{K}$ qui admettent une limite finie en a et :*

$$\begin{array}{rcl} \phi : A & \longrightarrow & \mathbb{K} \\ f & \longmapsto & \lim\limits_{x\to a} f(x) \end{array}$$

(i) A est un sous-espace vectoriel de $\mathcal{F}(I,\mathbb{K})$ et ϕ est une forme linéaire sur A ;

(ii) l'ensemble A_0 des fonctions de limite nulle en a est un sous-espace vectoriel de l'espace vectoriel A ;

(iii) si $f \in A_0$ (c'est-à-dire $\lim\limits_{x\to a} f(x) = 0$) et si g est bornée au voisinage de a, alors $f \times g \in A_0$;

(iv) A est un sous-anneau de $\mathcal{F}(I,\mathbb{K})$ et ϕ est un morphisme d'anneaux.

Preuve :

On traite le cas où $a \in \mathbb{R}$ par exemple.

• Montrons (i).

∗ Tout d'abord, $A \subset \mathcal{F}(I,\mathbb{K})$ et on constate que la fonction nulle est effectivement dans A (et même dans A_0).

∗ Ensuite, on montre que A est stable par combinaisons linéaires.

▷ Soit $(f,g) \in A^2$. On note $\ell \in \mathbb{K}$ et $\ell' \in \mathbb{K}$ les limites respectives de f et g en a. On fixe $\varepsilon > 0$. Alors, par définition de la limite :

$$\begin{array}{l} \exists \alpha_1 > 0 \ , \ \forall x \in I \ , \ |x-a| \leqslant \alpha_1 \Longrightarrow |f(x)-l| \leqslant \frac{\varepsilon}{2} \\ \exists \alpha_2 > 0 \ , \ \forall x \in I \ , \ |x-a| \leqslant \alpha_2 \Longrightarrow |g(x)-l| \leqslant \frac{\varepsilon}{2} \end{array}$$

On fixe un tel $\alpha_1 > 0$ et un tel $\alpha_2 > 0$, et on pose $\alpha = \min(\alpha_1, \alpha_2)$. On a alors $\alpha > 0$ et pour tout $x \in I$ tel que $|x-a| \leqslant \alpha$:

$$\begin{array}{rcl} |(f+g)(x) - (\ell+\ell')| & \leqslant & |f(x)-\ell| + |g(x)-\ell'| \\ & \leqslant & \dfrac{\varepsilon}{2} + \dfrac{\varepsilon}{2} \\ & \leqslant & \varepsilon \end{array}$$

Ceci prouve que $\lim\limits_{x\to a} ((f+g)(x)) = \ell + \ell'$, c'est-à-dire :

$$(f+g) \in A \quad \text{et} \quad \phi(f+g) = \phi(f) + \phi(g)$$

▷ Soient $f \in A$ et $\lambda \in \mathbb{K}$. Notons $\ell = \lim\limits_{x\to a} f(x) \in \mathbb{K}$.

Si $\lambda = 0$, alors $\lambda \cdot f = 0$ (fonction nulle) donc $\lambda \cdot f \in A$ et $\lim\limits_{x\to a} ((\lambda \cdot f)(x)) = 0 = \lambda \times \lim\limits_{x\to a} f(x)$.

On suppose à présent que $\lambda \neq 0$. Soit $\varepsilon > 0$. On applique la définition de la limite avec « $\varepsilon' = \dfrac{\varepsilon}{|\lambda|} > 0$ ». Il existe $\alpha > 0$ tel que :

$$\forall x \in I \cap [a-\alpha, a+\alpha] \ , \ |f(x) - \ell| \leqslant \varepsilon'$$

Il s'ensuit que :

$$\forall x \in I \cap [a-\alpha, a+\alpha] \ , \ |\lambda f(x) - \lambda\ell| \leqslant |\lambda||f(x) - \ell| \leqslant \varepsilon$$

Ce qui montre que $\lambda \cdot f \in A$ et $\phi(\lambda \cdot f) = \lambda \times \phi(f) = \lambda \cdot \phi(f)$.

Ainsi, on a montré que A est un sous-espace vectoriel de $\mathcal{F}(I, \mathbb{K})$ et :

$$\forall (f,g) \in A^2 \ , \ \forall \lambda \in \mathbb{K} \ , \ \phi(f+g) = \phi(f) + \phi(g) \text{ et } \phi(\lambda \cdot f) = \lambda \cdot \phi(f)$$

ϕ est donc une application $\mathbb{K}$-linéaire de A dans $\mathbb{K}$, c'est-à-dire une forme linéaire sur A.

• Montrons (ii).

Par définition, $A_0 = \ker(\phi)$ avec ϕ une application linéaire : A_0 est donc un sous-espace vectoriel de A.

Remarque : *en fait, ϕ est une forme linéaire non identiquement nulle donc A_0 est un hyperplan de A.*

• Montrons (iii).

Soient $f \in A_0$ et g une fonction bornée au voisinage de a. Par définition, il existe $\alpha_1 > 0$ et un réel $M > 0$ tels que :

$$\forall x \in I \cap [a-\alpha_1, a+\alpha_1] \ , \ |g(x)| \leqslant M$$

Par ailleurs, $\lim\limits_{x\to a} f(x) = 0$. Soit $\varepsilon > 0$, il existe $\alpha_2 > 0$ tel que :

$$\forall x \in I \cap [a-\alpha_2, a+\alpha_2] \ , \ |f(x)| \leqslant \frac{\varepsilon}{M}$$

Posons $\alpha = \min(\alpha_1, \alpha_2)$. On a alors $\alpha > 0$ et :

$$\forall x \in I \cap [a-\alpha, a+\alpha] \ , \ |(f \times g)(x)| \leqslant M|f(x)| \leqslant \varepsilon$$

Par conséquent, $\lim\limits_{x\to a} (f \times g)(x) = 0$, c'est-à-dire $f \times g \in A_0$.

• Montrons (iv).

$*$ $1_{\mathcal{F}(I,\mathbb{K})}$, la fonction constante égale à 1, appartient clairement à A et $\phi(1_{\mathcal{F}(I,\mathbb{K})}) = 1_{\mathbb{K}}$.

$*$ On a déjà montré que A est un $\mathbb{K}$-espace vectoriel et que ϕ est linéaire. Par suite,

▷ $\forall (f,g) \in A^2$, $(f-g) \in A$;

▷ $\forall (f,g) \in A^2$, $\phi(f+g) = \phi(f) + \phi(g)$.

$*$ Soit $(f,g) \in A^2$. Montrons que $f \times g \in A$ et $\phi(f \times g) = \phi(f) \times \phi(g)$. Soient $\ell = \lim\limits_{x\to a} f(x)$ et $\ell' = \lim\limits_{x\to a} g(x)$. On constate que pour tout $x \in I$:

$$(f \times g)(x) - \ell \times \ell' = f(x) \times (g(x) - \ell') + \ell' \times (f(x) - \ell)$$

Or, $(g-\ell') \in A_0$ et f bornée au voisinage de a (puisque f admet une limite finie en a) donc d'après (iii), $f \times (g-\ell') \in A_0$. De même, $\ell' \times (f-\ell) \in A_0$. Or, d'après (ii), A_0 est un espace vectoriel. Par suite, $(f \times g - \ell \times \ell') \in A_0$, c'est-à-dire :

$$f \times g \in A$$

et

$$\lim_{x\to a} (f(x) \times g(x)) = \ell \times \ell'$$

soit encore

$$\lim_{x\to a} (f(x) \times g(x)) = \lim_{x\to a} f(x) \times \lim_{x\to a} g(x)$$

Ce qui montre que $\phi(f \times g) = \phi(f) \times \phi(g)$.

⊠

Remarques :

- *en clair, cette proposition affirme qu'un produit ou une combinaison linéaire de fonctions admettant des limites finies en a a aussi une limite finie en a et que sa limite s'obtient comme produit ou combinaison linéaire des limites respectives. Cette proposition dit aussi qu'un produit d'une fonction bornée au voisinage de a et d'une fonction qui tend vers 0 est une fonction qui tend vers 0 ;*
- *on reverra des méthodes plus « simples » pour établir ces propriétés en utilisant la caractérisation séquentielle de la limite. En effet, cette caractérisation nous permettra de déduire toutes ces propriétés des mêmes propriétés pour les suites.*

Proposition 6.2.3.2 *Soient $f : I \longrightarrow \mathbb{K}$ et $a \in \overline{I}$. Si f admet une limite finie non nulle ℓ en a, alors $\dfrac{1}{f}$ admet une limite finie en a et $\lim\limits_{x\to a} \dfrac{1}{f(x)} = \dfrac{1}{\ell}$.*

Preuve :

On fait la démonstration pour $a = -\infty$. Pour commencer, on montre que $\frac{1}{f}$ est bien définie au voisinage de a. Posons $\varepsilon = \frac{|\ell|}{2} > 0$ (puisque $\ell \neq 0$). Puisque $\lim\limits_{x\to-\infty} f(x) = \ell$, il existe $B \in \mathbb{R}$ tel que :

$$\forall x \in I \cap]-\infty, B] \ , \ |f(x) - \ell| \leqslant \varepsilon$$

Soit $x \in I \cap]-\infty, B]$. On a alors : $|\ell| - |f(x)| \leqslant |\ell - f(x)| \leqslant \varepsilon$, c'est-à-dire $|f(x)| \geqslant |\ell| - \varepsilon > 0$. Ceci montre que $\frac{1}{|f|}$ est bien définie pour $x \in I \cap]-\infty, B]$ et que $\frac{1}{|f|}$ est bornée au voisinage de $-\infty$.
Mais alors, $|\frac{1}{f} - \frac{1}{\ell}| = \frac{|f-\ell|}{|\ell|\times|f|}$ est le produit d'une fonction bornée au voisinage de a (la fonction $\frac{1}{|\ell|\times|f|}$) et d'une fonction qui tend vers 0 (la fonction $|f - \ell|$). D'après la proposition précédente, $\lim\limits_{x\to a} \left|\dfrac{1}{f(x)} - \dfrac{1}{\ell}\right| = 0$.

⊠

Corollaire 6.2.3.3 *Soient f et g admettant une limite finie en a et $\lim\limits_{x\to a} g(x) \neq 0$. Alors $\dfrac{f}{g}$ admet une limite finie en a et*

$$\lim_{x\to a} \left(\frac{f(x)}{g(x)}\right) = \frac{\lim\limits_{x\to a} f(x)}{\lim\limits_{x\to a} g(x)}$$

On peut traduire ce que l'on vient d'énoncer et compléter avec les règles de calcul dans $\overline{\mathbb{R}}$: **pour $\mathbf{f, g : I \longrightarrow \mathbb{R}}$ et $a \in \overline{I}$,**

Limite d'une somme

$\lim\limits_{x\to a} f(x)$	ℓ	ℓ ou $+\infty$	ℓ ou $-\infty$	$+\infty$
$\lim\limits_{x\to a} g(x)$	ℓ'	$+\infty$	$-\infty$	$-\infty$
$\lim\limits_{x\to a} (f+g)(x)$	$\ell + \ell'$	$+\infty$	$-\infty$	? ? ?

Limite d'un produit

$\lim\limits_{x\to a} f(x)$	ℓ	$\ell>0$ ou $+\infty$	$\ell<0$ ou $-\infty$	$\ell>0$ ou $+\infty$	$\ell<0$ ou $-\infty$	0
$\lim\limits_{x\to a} g(x)$	ℓ'	$+\infty$	$+\infty$	$-\infty$	$-\infty$	$\pm\infty$
$\lim\limits_{x\to a} (f\times g)(x)$	$\ell\times\ell'$	$+\infty$	$-\infty$	$-\infty$	$+\infty$	???

Limite de l'inverse d'une fonction

$\lim\limits_{x\to a} f(x)$	$\ell\neq 0$	$\ell=0$ et $f>0$	$\ell=0$ et $f<0$	$\pm\infty$
$\lim\limits_{x\to a} \dfrac{1}{f(x)}$	$\dfrac{1}{\ell}$	$+\infty$	$-\infty$	0

Remarques :

- *dans ces tableaux, la notation ??? signifie qu'il s'agit d'une forme indéterminée, c'est-à-dire qu'on ne peut pas conclure en général : cela dépend des fonctions ;*
- *on en déduit les règles pour le quotient de deux fonctions en écrivant :* $\dfrac{f}{g} = f\times\dfrac{1}{g}$ *et en appliquant les règles de l'inverse et du produit.*

Pour les fonctions à valeurs complexes, c'est encore plus simple puisqu'il n'y a pas de limite infinie ! Si une fonction à valeurs complexes admet une limite, elle est nécessairement finie. Ainsi, **pour $\mathbf{f,g : I\longrightarrow\mathbb{C}}$ et $\mathbf{a\in\overline{I}}$:**

$$\left\{\begin{array}{rcl}\lim\limits_{x\to a} f(x) &=& \ell\in\mathbb{C}\\ \lim\limits_{x\to a} g(x) &=& \ell'\in\mathbb{C}\end{array}\right. \Longrightarrow \left\{\begin{array}{rcl}\lim\limits_{x\to a} (f+g)(x) &=& \ell+\ell'\\ \lim\limits_{x\to a} (f\times g)(x) &=& \ell\times\ell'\\ \lim\limits_{x\to a} \left(\dfrac{f(x)}{g(x)}\right) &=& \dfrac{\ell}{\ell'} \text{ si } \ell'\neq 0\end{array}\right.$$

Remarque : *parmi les résultats donnés dans les tableaux, tous n'ont pas encore été démontrés. À titre d'exemple, on va en prouver un. Les autres sont laissés en exercice.*

Exemple 6.2.3.4 Montrons que si $\lim\limits_{x\to a} f(x) = \ell \in \mathbb{R}$ et $\lim\limits_{x\to a} g(x) = -\infty$, alors :

$$\lim_{x\to a} (f+g)(x) = -\infty$$

Soit $A \in \mathbb{R}$. Puisque $\lim\limits_{x\to a} g(x) = -\infty$, il existe un voisinage V_1 de a tel que :

$$\forall x \in I \cap V_1 \ , \ g(x) \leqslant A - \ell - 1$$

De plus, puisque $\lim\limits_{x\to a} f(x) = \ell$, il existe un voisinage V_2 de a tel que :

$$\forall x \in I \cap V_2 \ , \ |f(x) - \ell| \leqslant 1$$

Il s'ensuit que pour tout $x \in I \cap (V_1 \cap V_2)$,

$$(f+g)(x) = f(x) + g(x) \leqslant \ell + 1 + g(x) \leqslant \ell + 1 + A - \ell - 1 \leqslant A$$

Ce qui prouve que $\lim\limits_{x\to a} (f+g)(x) = -\infty$.

Exercice 6.2.3.5 On sait que si $\lim\limits_{x\to a} f(x) = +\infty$ et $\lim\limits_{x\to a} g(x) = -\infty$, alors les limites de $f+g$ et $\dfrac{f}{g}$ sont des formes indéterminées.
Donner des exemples de fonctions f et g telles que $\lim\limits_{x\to a} f(x) = +\infty$, $\lim\limits_{x\to a} g(x) = -\infty$ et :

1. $f+g$ n'admet pas de limite ;
2. $f+g$ admet $+\infty$ (respectivement $-\infty$) pour limite ;
3. $f+g$ admet le nombre $\ell \in \mathbb{R}$ pour limite ;
4. $\dfrac{f}{g}$ n'a pas de limite.

Corollaire 6.2.3.6 *L'ensemble des fonctions continues en a est un sous-anneau et sous-espace vectoriel de A. De plus, si $g(a) \neq 0$ et f et g sont continues en a, alors f/g est aussi continue en a.*

Preuve :

Ceci découle directement des propriétés algébriques des limites et de la définition de la continuité.

⊠

6.2.4 Compatibilité du passage à la limite avec la relation d'ordre dans $\mathbb{R}$

Théorème 6.2.4.1 *Soient f et g deux applications de I dans $\mathbb{R}$, et $a \in \overline{I}$. On suppose que $f \leqslant g$ au voisinage de a.*

(i) Si $\lim_{x\to a} f(x) = +\infty$, alors g admet une limite en a et $\lim_{x\to a} g(x) = +\infty$.

(ii) Si $\lim_{x\to a} g(x) = -\infty$, alors f admet une limite en a et $\lim_{x\to a} f(x) = -\infty$.

(iii) Si f et g admettent des limites en a, alors $\lim_{x\to a} f(x) \leqslant \lim_{x\to a} g(x)$ (dans $\overline{\mathbb{R}}$).

Preuve :

• Montrons (i).
On suppose que $\lim_{x\to a} f(x) = +\infty$. Montrons que $\lim_{x\to a} g(x) = +\infty$.

∗ Pour commencer, on sait que $f \leqslant g$ au voisinage de a, c'est-à-dire qu'il existe V_1 un voisinage de a tel que :

$$\forall x \in I \cap V_1 \ , \ f(x) \leqslant g(x)$$

∗ Soit $A \in \mathbb{R}$. Puisque $\lim_{x\to a} f(x) = +\infty$, il existe V_2 un voisinage de a tel que :

$$\forall x \in I \cap V_2 \ , \ A \leqslant f(x)$$

Posons $V = V_1 \cap V_2$. Alors V est un voisinage de a et :

$$\forall x \in I \cap V \ , \ g(x) \geqslant f(x) \geqslant A$$

Ce qui prouve que $\lim_{x\to a} g(x) = +\infty$.

• La propriété (ii) s'obtient en appliquant (i) au couple $(-g, -f)$.

• Montrons enfin (iii).
On suppose que f et g ont des limites (finies ou infinies en a) et on note $\lim_{x\to a} f(x) = \ell \in \overline{\mathbb{R}}$ et $\lim_{x\to a} g(x) = \ell' \in \overline{\mathbb{R}}$.

∗ Si $\ell = -\infty$ ou $\ell' = +\infty$, alors l'inégalité $\ell \leqslant \ell'$ est toujours vraie dans $\overline{\mathbb{R}}$.

∗ Si $\ell = +\infty$ (ou $\ell' = -\infty$) alors d'après (i) (ou (ii)) $\ell' = +\infty$ (ou $\ell = -\infty$) et donc $\ell \leqslant \ell'$.

∗ Il reste donc à traiter le cas où $(\ell, \ell') \in \mathbb{R}^2$, c'est-à-dire le cas où f et g admettent des limites finies en a.

On rédige la preuve dans le cas $a = +\infty$. Soit $\varepsilon > 0$.

▷ $f \leqslant g$ au voisinage de $a = +\infty$ donc il existe $A_1 \in \mathbb{R}$ tel que :

$$\forall x \in I \cap [A_1, +\infty[\ ,\ f(x) \leqslant g(x)$$

▷ $\lim\limits_{x\to a} f(x) = \ell \in \mathbb{R}$ donc il existe $A_2 \in \mathbb{R}$ tel que :

$$\forall x \in I \cap [A_2, +\infty[\ ,\ \ell - \varepsilon \leqslant f(x) \leqslant \ell + \varepsilon$$

▷ $\lim\limits_{x\to a} g(x) = \ell' \in \mathbb{R}$ donc il existe $A_3 \in \mathbb{R}$ tel que :

$$\forall x \in I \cap [A_3, +\infty[\ ,\ \ell' - \varepsilon \leqslant g(x) \leqslant \ell' + \varepsilon$$

On choisit alors $x_0 \in I$ tel que $x_0 \geqslant \max(A_1, A_2, A_3)$ (ce qui est possible car $\sup I = +\infty$ et I est un intervalle d'intérieur non vide). Alors :

$$\ell - \varepsilon \leqslant f(x_0) \leqslant g(x_0) \leqslant \ell' + \varepsilon$$

Ainsi, on a montré que : $\forall \varepsilon > 0\ ,\ \ell \leqslant \ell' + 2\varepsilon$. Par suite, $\ell \leqslant \ell'$.

⊠

Remarques :

- *à nouveau pour éviter les confusions, il est préférable d'appliquer (iii) lorsque f et g ont des limites finies ;*
- *lorsqu'on applique (iii), il ne faut pas oublier de justifier avant l'existence des limites ;*
- *dans la rédaction, on écrira souvent « $f \leqslant g$. Or f et g ont des limites finies en a, on peut donc passer à la limite dans l'inégalité, ce qui donne : ... ».*

Exemple 6.2.4.2 Soit $g : \mathbb{R} \longrightarrow \mathbb{R}$ définie par : $\forall x \in \mathbb{R}\ ,\ g(x) = x + \sin(x)$.
Pour tout réel x, $x-1 \leqslant g(x)$ et $\lim\limits_{x\to+\infty} (x-1) = +\infty$. Par comparaison, $\lim\limits_{x\to+\infty} g(x) = +\infty$.

⚠ **Attention :** de même que pour les suites, le passage à la limite ne conserve pas les inégalités strictes ! Autrement dit :

$$\Big(f < g \text{ et } f, g \text{ ont des limites finies en } a\Big) \not\Longrightarrow \lim_{x\to a} f(x) < \lim_{x\to a} g(x)$$

Par exemple, pour tout $x \in \mathbb{R}$, $0 < \frac{1}{1+x^2}$, $f : x \longmapsto 0$ admet une limite finie en $+\infty$, $g : x \longmapsto \frac{1}{1+x^2}$ admet une limite finie en $+\infty$ mais $\lim\limits_{x\to+\infty} f(x) = \lim\limits_{x\to+\infty} g(x)$.

Théorème 6.2.4.3 (Théorème des gendarmes) *Soient f, g, h trois fonctions de I dans $\mathbb{R}$ et $a \in \overline{I}$. On suppose que :*

(1) au voisinage de a, $f \leqslant g \leqslant h$;

(2) f et h ont des limites finies en a ;

(3) $\lim\limits_{x\to a} f(x) = \lim\limits_{x\to a} h(x) = \ell$.

Alors :

(i) g a une limite finie en a ;

(ii) et $\lim\limits_{x\to a} g(x) = \ell$.

Preuve :

On fait la preuve dans le cas $a \in \mathbb{R} \cap \overline{I}$ (sinon utiliser des voisinages pour le cas général). Soit $\varepsilon > 0$.

- D'après les hypothèses, $\lim\limits_{x\to a} f(x) = \ell$ donc :

$$\exists \alpha_1 > 0 \ , \forall x \in I \cap [a - \alpha_1, a + \alpha_1] \ , \ |f(x) - \ell| \leqslant \varepsilon$$

- De même, $\lim\limits_{x\to a} h(x) = \ell$ donc :

$$\exists \alpha_2 > 0 \ , \forall x \in I \cap [a - \alpha_2, a + \alpha_2] \ , \ |h(x) - \ell| \leqslant \varepsilon$$

- Enfin $f \leqslant g \leqslant h$ au voisinage de a donc :

$$\exists \alpha_3 > 0 \ , \forall x \in I \cap [a - \alpha_3, a + \alpha_3] \ , \ f(x) \leqslant g(x) \leqslant h(x)$$

Soient de tels réels α_1, α_2 et α_3. On pose $\alpha = \min(\alpha_1, \alpha_2, \alpha_3)$ (ce qui garantit que les trois inégalités seront valables si $x \in I \cap [a - \alpha, a + \alpha]$). Alors $\alpha > 0$ et :

$$\forall x \in I \cap [a - \alpha, a + \alpha] \ , \ \ell - \varepsilon \leqslant f(x) \leqslant g(x) \leqslant h(x) \leqslant \ell + \varepsilon$$

Ce qui montre que $\lim\limits_{x\to a} g(x) = \ell$.

⊠

Remarque : *bien que le résultat de ce théorème soit encore valable lorsque $\ell = +\infty$ ou $\ell = -\infty$, ce n'est plus le théorème des gendarmes ! C'est simplement le théorème de comparaison que l'on a vu juste avant.*

Exemple 6.2.4.4 On sait que[1] pour tout $x > 0$, $x - \frac{x^3}{6} \leqslant \sin(x) \leqslant x$. Alors, pour tout $x > 0$,

$$1 - \frac{x^2}{6} \leqslant \frac{\sin(x)}{x} \leqslant 1$$

Or, $\lim\limits_{\substack{x\to 0\\ x>0}} \left(1 - \frac{x^2}{6}\right) = \lim\limits_{\substack{x\to 0\\ x>0}} 1 = 1$. D'après le théorème des gendarmes, $x \longmapsto \frac{\sin(x)}{x}$ admet une limite finie à droite en 0 et :

$$\lim_{\substack{x\to 0\\ x>0}} \frac{\sin(x)}{x} = 1$$

De même que pour les suites, le théorème des gendarmes est un outil très important dans la recherche de limite et/ou d'équivalents de fonctions.

Exemple 6.2.4.5 On considère la fonction f définie sur $]0, +\infty[$ par :

$$\forall x \in]0, +\infty[\ , \ f(x) = \int_0^{\frac{\pi}{2}} \frac{\cos(t)}{t^2 + x^2} \, \mathrm{d}t$$

• On peut noter que f est bien définie sur $]0, +\infty[$ puisque pour tout $x > 0$, la fonction $t \longmapsto \frac{\cos(t)}{t^2 + x^2}$ est continue[2] sur le segment $[0, \frac{\pi}{2}]$.

• On peut aussi remarquer qu'on ne connaît pas de primitive de $t \longmapsto \frac{\cos(t)}{t^2+x^2}$ et qu'on ne peut donc pas déterminer l'expression explicite de f pour calculer les limites aux bornes de son ensemble de définition. On va donc essayer d'encadrer la fonction f de façon assez précise pour pourvoir trouver les limites puis les équivalents.

• Étude lorsque x tend vers $+\infty$.

∗ Dans un premier temps, pour $x > 0$, on a :

$$\forall t \in [0, \frac{\pi}{2}] \ , \ 0 \leqslant \frac{\cos(t)}{t^2 + x^2} \leqslant \frac{1}{x^2}$$

Par croissance de l'intégrale :

$$\int_0^{\frac{\pi}{2}} 0 \, \mathrm{d}t \leqslant \int_0^{\frac{\pi}{2}} \frac{\cos(t)}{t^2 + x^2} \, \mathrm{d}t \leqslant \int_0^{\frac{\pi}{2}} \frac{1}{x^2} \, \mathrm{d}t$$

c'est-à-dire

$$0 \leqslant f(x) \leqslant \frac{\pi}{2x^2}$$

1. sinon, on peut faire l'étude de fonction pour le prouver.
2. on admet ici les propriétés simples sur la continuité et l'intégration qui seront vues dans le cours de mathématiques supérieures 2.

Or, $\lim\limits_{x\to+\infty} \dfrac{\pi}{2x^2} = 0$ donc d'après le théorème des gendarmes :

$$\lim_{x\to+\infty} f(x) = 0$$

$*$ On souhaite maintenant déterminer un équivalent de f en $+\infty$ (si vous avez oublié la notion informelle d'équivalent, vous pouvez d'abord lire le paragraphe 3 de ce chapitre puis revenir à cet exemple mais il n'est pas nécessaire de maîtriser la théorie pour suivre la démarche de cet exemple).
L'encadrement précédent permet de trouver la limite mais il ne permet pas de trouver un équivalent car les termes avec lesquels on a encadré f ne sont du même ordre de grandeur. On va donc refaire un encadrement un peu plus précis. En reprenant la même démarche qu'avant, on a successivement pour tout $x > 0$:

$$\forall t \in [0, \frac{\pi}{2}] \ , \ \frac{\cos(t)}{\frac{\pi^2}{4} + x^2} \leqslant \frac{\cos(t)}{x^2 + t^2} \leqslant \frac{\cos(t)}{x^2}$$

et donc

$$\frac{1}{\frac{\pi^2}{4} + x^2} \int_0^{\frac{\pi}{2}} \cos(t)\,\mathrm{d}t \leqslant f(x) \leqslant \frac{1}{x^2} \int_0^{\frac{\pi}{2}} \cos(t)\,\mathrm{d}t$$

soit encore, compte-tenu du fait que $\int_0^{\frac{\pi}{2}} \cos(t)\,\mathrm{d}t = [\sin(t)]_0^{\frac{\pi}{2}} = 1$,

$$\frac{1}{\frac{\pi^2}{4} + x^2} \leqslant f(x) \leqslant \frac{1}{x^2}$$

Il s'ensuit que :

$$\forall x > 0 \ , \ \frac{1}{1 + \frac{\pi^2}{4x^2}} \leqslant x^2 f(x) \leqslant 1$$

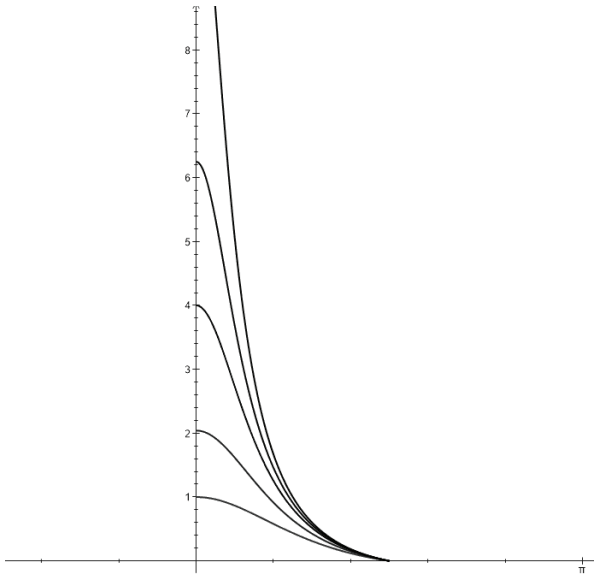
Or, $\lim\limits_{x\to+\infty} \dfrac{1}{1 + \frac{\pi^2}{4x^2}} = 1$ donc, d'après le théorème des gendarmes,

$$\lim_{x\to+\infty} x^2 f(x) = 1 \quad \text{c'est-à-dire} \quad f(x) \underset{x\to+\infty}{\sim} \frac{1}{x^2}$$

• Étudions à présent le comportement de f au voisinage de 0.

$*$ Commençons par déterminer la limite de f. Je vous laisse vérifier que les inégalités obtenues avant ne permettent pas de trouver la limite de f en 0 (puisque dans chaque encadrement, le minorant a une limite finie en 0 et le majorant tend vers $+\infty$).

Pour essayer de comprendre le comportement de la fonction f, on trace la courbe représentative de $t \longmapsto \frac{\cos(t)}{t^2+x^2}$ pour des valeurs de x de plus en plus « petites » :



Graphiquement, on semble constater que c'est l'aire au voisinage de $t = 0$ qui devient de plus en plus importante et elle semble tendre vers $+\infty$ lorsque x tend vers 0. On cherche donc à minorer la fonction f. Pour cela, on doit minorer la fonction cos. Sur l'intervalle $[0, \frac{\pi}{2}]$, la seule minoration possible est 0, ce qui ne permet évidemment pas de conclure. Or, comme on a conjecturé que c'est au voisinage de $t = 0$ que l'aire est importante, on peut simplement regarder l'intégrale sur un intervalle plus petit, « proche de 0 ».
Pour tout $x > 0$, $t \longmapsto \frac{\cos(t)}{t^2+x^2}$ est positive sur $[0, \frac{\pi}{2}]$, par suite :

$$f(x) = \int_0^{\frac{\pi}{2}} \frac{\cos(t)}{t^2+x^2}\,\mathrm{d}t \geqslant \int_0^{\frac{\pi}{3}} \frac{\cos(t)}{t^2+x^2}\,\mathrm{d}t$$

Maintenant, sur l'intervalle $[0, \frac{\pi}{3}]$, on peut minorer la fonction cosinus par $\frac{1}{2}$, ce qui donne :

$$f(x) \geqslant \frac{1}{2}\int_0^{\frac{\pi}{3}} \frac{1}{t^2+x^2}\,\mathrm{d}t = \frac{1}{2}\left[\frac{1}{x}\arctan\left(\frac{t}{x}\right)\right]_0^{\frac{\pi}{3}}$$

soit encore :

$$f(x) \geqslant \frac{1}{2x}\arctan\left(\frac{\pi}{3x}\right)$$

Or, $\lim\limits_{\substack{x\to 0\\ x>0}} \arctan\left(\frac{\pi}{3x}\right) = \frac{\pi}{2} > 0$ et $\lim\limits_{\substack{x\to 0\\ x>0}} \frac{1}{2x} = +\infty$. Par comparaison :

$$\lim_{\substack{x\to 0\\ x>0}} f(x) = +\infty$$

$*$ Pour trouver un équivalent maintenant, il va falloir être plus précis. Au voisinage de $t=0$, on sait que $\cos(t)\sim 1$. On va donc comparer f et $x\longmapsto \displaystyle\int_0^{\frac{\pi}{2}} \frac{1}{t^2+x^2}\,\mathrm{d}t$.
Soit $x>0$.

$$\begin{aligned}\left|f(x)-\int_0^{\frac{\pi}{2}}\frac{1}{t^2+x^2}\,\mathrm{d}t\right| &= \int_0^{\frac{\pi}{2}}\frac{1-\cos(t)}{t^2+x^2}\,\mathrm{d}t\\ &= \int_0^{\frac{\pi}{2}}\frac{2\sin^2(\frac{t}{2})}{t^2+x^2}\,\mathrm{d}t\\ &\leqslant \int_0^{\frac{\pi}{2}}\frac{2(\frac{t}{2})^2}{t^2+x^2}\,\mathrm{d}t\\ &\leqslant \int_0^{\frac{\pi}{2}}\frac{t^2}{2(t^2+x^2)}\,\mathrm{d}t\\ &\leqslant \int_0^{\frac{\pi}{2}}\frac{1}{2}\,\mathrm{d}t\\ &\leqslant \frac{\pi}{4}\end{aligned}$$

Or, $\displaystyle\int_0^{\frac{\pi}{2}}\frac{1}{t^2+x^2}\,\mathrm{d}t=\left[\frac{1}{x}\arctan\left(\frac{t}{x}\right)\right]_0^{\frac{\pi}{2}}=\frac{1}{x}\arctan\left(\frac{\pi}{2x}\right)$. Ainsi, pour tout $x>0$,

$$-\frac{\pi}{4}\leqslant f(x)-\frac{1}{x}\arctan\left(\frac{\pi}{2x}\right)\leqslant\frac{\pi}{4}$$

soit encore,

$$\arctan\left(\frac{\pi}{2x}\right)-\frac{\pi x}{4}\leqslant xf(x)\leqslant\arctan\left(\frac{\pi}{2x}\right)+\frac{\pi x}{4}$$

Or, $\displaystyle\lim_{\substack{x\to 0\\ x>0}}\left(\arctan\left(\frac{\pi}{2x}\right)-\frac{\pi x}{4}\right)=\frac{\pi}{2}$ et de même, $\displaystyle\lim_{\substack{x\to 0\\ x>0}}\left(\arctan\left(\frac{\pi}{2x}\right)+\frac{\pi x}{4}\right)=\frac{\pi}{2}$. D'après le théorème des gendarmes,

$$\lim_{\substack{x\to 0\\ x>0}} xf(x)=\frac{\pi}{2}\quad\text{c'est-à-dire}\quad f(x)\underset{x\to 0^+}{\sim}\frac{\pi}{2x}$$

Remarque : *il y a d'autres méthodes plus « simples » qui permettent de trouver ces équivalents mais qui nécessitent des outils un peu plus avancés en intégration (voir cours de mathématiques spéciales 2). Les études de fonctions f de cette forme ne sont pas un objectif pour ce livre.*

On peut terminer avec le corollaire suivant, très pratique, et conséquence immédiate du théorème des gendarmes.

Corollaire 6.2.4.6 *Si $|f|\leqslant g$ au voisinage de a et si $\lim\limits_{x\to a} g(x)=0$, alors $\lim\limits_{x\to a} f(x)=0$.*

6.2.5 Composition de limites et caractérisation séquentielle de la limite

Proposition 6.2.5.1 *Soient $f : I \longrightarrow J \subset \mathbb{R}$ et $g : J \longrightarrow \mathbb{K}$ deux fonctions, $a \in \overline{I}$. On suppose que :*

1. $\lim\limits_{x\to a} f(x) = \ell \in \overline{\mathbb{R}}$;
2. $\lim\limits_{x\to \ell} g(x) = L$.

Alors $g \circ f$ admet une limite en a et $\lim\limits_{x\to a} (g \circ f)(x) = L$.

Preuve :

On veut montrer que :

$$\forall U \in \mathcal{V}_f(L) \ , \ \exists W \in \mathcal{V}_f(a) \ , \ \forall x \in I \cap W \ , \ (g \circ f)(x) \in U$$

Soit $U \in \mathcal{V}_f(L)$. Par hypothèse, $\lim\limits_{y\to \ell} g(y) = L$. Il existe $V \in \mathcal{V}_f(\ell)$ tel que :

$$\forall y \in J \cap V \ , \ g(y) \in U$$

Par ailleurs, $\lim\limits_{x\to a} f(x) = \ell$: par conséquent, il existe $W \in \mathcal{V}_f(a)$ tel que :

$$\forall x \in I \cap W \ , \ f(x) \in V$$

Soit $x \in I \cap W$. Alors $f(x) \in V$ et par définition, $f(x) \in J$. Par suite, $f(x) \in J \cap V$. Il s'ensuit que :

$$\forall x \in I \cap W \ , \ g(f(x)) \in U$$

Ce qui prouve que $\lim\limits_{x\to a} (g \circ f)(x) = L$.

⊠

Remarques :

- *il est très important de retenir les hypothèses précises de ce théorème : en particulier, on ne fait aucune hypothèse de régularité sur les fonctions f et g ! On suppose uniquement que $g \circ f$ est bien définie, que f a une limite ℓ (finie ou infinie) en a et que g a une limite (finie ou infinie) en $L = \lim\limits_{x\to a} f(x)$;*
- *on a supposé ici que f est à valeurs réelles car nous n'avons pas encore étudié la notion de limite pour une fonction d'une variable complexe. La continuité de ce type de fonctions est étudiée dans le cours de mathématiques spéciales 1 (espaces vectoriels normés).*

Théorème 6.2.5.2 (Caractérisation séquentielle de la limite)

Soient $f : I \longrightarrow \mathbb{K}$, $a \in \overline{I}$ et $\ell \in \mathbb{K}$ (ou $\ell \in \overline{\mathbb{R}}$ si $\mathbb{K} = \mathbb{R}$). Alors les propriétés suivantes sont équivalentes :

(i) $\lim\limits_{x \to a} f(x) = \ell$;

(ii) pour toute suite $(u_n)_{n\in\mathbb{N}} \in I^{\mathbb{N}}$ admettant a pour limite, $(f(u_n))_{n\in\mathbb{N}}$ admet ℓ pour limite.

On dit que la propriété (ii) est la caractérisation séquentielle (ou par les suites) de la limite.

Preuve :

• $(i) \implies (ii)$ découle du théorème de composition des limites. Néanmoins, comme ce théorème a été énoncé pour des fonctions d'une variable réelle (et pas pour des suites), on refait la démonstration.

On suppose (i), c'est-à-dire f admet ℓ pour limite en a. Montrons (ii).
Soit $(u_n)_{n\in\mathbb{N}}$ une suite d'éléments de I, de limite a. Montrons que $(f(u_n))_{n\in\mathbb{N}}$ admet ℓ pour limite.
Soit $U \in \mathcal{V}_f(\ell)$. Par hypothèse, $\lim\limits_{x\to a} f(x) = \ell$: il existe donc un voisinage $V \in \mathcal{V}_f(a)$ tel que :

$$\forall x \in I \cap V \ , \ f(x) \in U$$

Par ailleurs, $\lim\limits_{n\to+\infty} u_n = a$ donc il existe $n_0 \in \mathbb{N}$ tel que :

$$\forall n \geqslant n_0 \ , \ u_n \in V$$

On a alors : $\forall n \geqslant n_0 \ , \ f(u_n) \in U$.

Ce qui prouve que la suite $(f(u_n))_{n\in\mathbb{N}}$ admet ℓ pour limite.

• Montrons $(ii) \implies (i)$ par contraposée.

On suppose non (i), et on montre non (ii). Par hypothèse, ℓ n'est pas la limite de f en a, c'est-à-dire :

$$(\star) \quad \exists U \in \mathcal{V}_f(l) \ , \ \forall V \in \mathcal{V}_f(a) \ , \ \exists x \in I \cap V \ , \ f(x) \notin U$$

On fixe un tel voisinage U. Soit $n \in \mathbb{N}$. On pose :

$$V_n = \begin{cases} [a - \frac{1}{n+1}, a + \frac{1}{n+1}] & \text{si } a \in \mathbb{R} \\ [n, +\infty[& \text{si } a = +\infty \\ ]-\infty, -n] & \text{si } a = -\infty \end{cases}$$

Alors $V_n \in \mathcal{V}_f(a)$ donc d'après $(\star)$, il existe $x_n \in I \cap V_n$ tel que $f(x_n) \notin U$. On choisit un tel x_n. Ceci définit une suite $(x_n)_{n\in\mathbb{N}}$ d'éléments de I telle que :

* Pour tout entier $n \in \mathbb{N}$,

$$x_n \in \begin{cases} [a - \frac{1}{n+1}, a + \frac{1}{n+1}] & \text{si } a \in \mathbb{R} \\ [n, +\infty[& \text{si } a = +\infty \\ ]-\infty, -n] & \text{si } a = -\infty \end{cases}$$

D'après le théorème de comparaison (ou le théorème des gendarmes lorsque $a \in \mathbb{R}$) $\lim\limits_{n\to+\infty} x_n = a$;

* $\forall n \in \mathbb{N}$, $f(x_n) \notin U$.

Par conséquent, on a montré qu'il existe une suite d'éléments de I, admettant a pour limite, et telle que $(f(x_n))_{n\in\mathbb{N}}$ n'admet pas ℓ pour limite, c'est-à-dire non (ii).

⊠

Exercice 6.2.5.3 Refaire la démonstration lorsque $a \in \mathbb{R}$ et $\ell = +\infty$.

Remarque fondamentale : *dans ce théorème, l'hypothèse (i) est une hypothèse « continue » (le x tend vers a mais x est un réel) alors que l'hypothèse (ii) est une hypothèse « discrète » (en chaque point x_n de la suite). Dans de nombreux domaines mathématiques ou dispose de caractérisations séquentielles : c'est pratique car cela permet de manipuler des suites qui sont des objets « plus familiers ». Dans toutes les démonstrations de ce type de caractérisation, on retient que :*

« continu » $\implies$ « discret » (toujours simple et se prouve directement)

« discret » $\implies$ « continu » (toujours par contraposée)

Vous devez retenir que les réciproques se prouvent toujours par contraposée. Intuitivement c'est facile à comprendre car une « information ponctuelle » (c'est-à-dire discrète) ne se traduit pas par une « information continue ».

Remarques :

- *dans l'énoncé du théorème, notez bien qu'on dit « $(u_n)_{n\in\mathbb{N}}$ admet a pour limite » et non « $(u_n)_{n\in\mathbb{N}}$ converge vers a » (et de même pour $(f(u_n))_{n\in\mathbb{N}}$) : c'est parce que le théorème est valable lorsque $a = +\infty$ (ou $a = -\infty$). Lorsque $a \in \mathbb{R}$, bien entendu on peut remplacer « admet a pour limite » par « converge vers a » ;*
- *on aurait pu commencer par cette caractérisation de la limite pour ensuite en déduire les propriétés algébriques et la compatibilité du passage à la limite avec la relation d'ordre dans $\mathbb{R}$ à partir des mêmes propriétés déjà établies pour les suites ;*

- *dans un cadre pratique, on utilise la caractérisation séquentielle de la limite pour montrer qu'une fonction n'admet pas de limite mais rarement pour prouver qu'elle admet une limite ;*
- *dans un cadre plus théorique, c'est souvent plus facile d'utiliser la caractérisation séquentielle pour prouver l'existence d'une limite.*

Exemple 6.2.5.4 Montrons que cos n'a pas de limite en $+\infty$. Soit $(x_n)_{n\in\mathbb{N}}$ définie par $x_n = n\pi$ pour tout entier n. Alors :

- $(x_n)_{n\in\mathbb{N}}$ tend vers $+\infty$ c'est-à-dire $(x_n)_{n\in\mathbb{N}}$ admet $+\infty$ pour limite ;
- mais $(\cos(x_n))_{n\in\mathbb{N}} = ((-1)^n)_{n\in\mathbb{N}}$ n'a pas de limite.

On a donc trouvé une suite $(x_n)_{n\in\mathbb{N}}$ de limite $+\infty$ telle que la suite $(\cos(x_n))_{n\in\mathbb{N}}$ n'a pas de limite. D'après la caractérisation séquentielle de la limite, cos n'a pas de limite en $+\infty$.

Remarque : *il est parfois plus simple de donner deux suites $(x_n)_{n\in\mathbb{N}}$ et $(y_n)_{n\in\mathbb{N}}$ de limite a telles que $(f(x_n))$ et $(f(y_n))$ ont des limites différentes : cela permet également de conclure que f n'a pas de limite en a.*

Exemple 6.2.5.5 Montrons que $\chi_{\mathbb{Q}}$ n'a pas de limite en $+\infty$.

- Soit $(x_n) = (n)$. Alors $\lim\limits_{n\to+\infty} x_n = +\infty$ et $\lim\limits_{n\to+\infty} \chi_{\mathbb{Q}}(x_n) = 1$ (puisque pour tout entier $n \in \mathbb{N}$, $\chi_{\mathbb{Q}}(n) = 1$) ;
- Soit $(y_n) = (n\sqrt{2})$. Alors $\lim\limits_{n\to+\infty} y_n = +\infty$ et $\lim\limits_{n\to+\infty} \chi_{\mathbb{Q}}(x_n) = 0$ (puisque pour tout entier $n \in \mathbb{N}$, $\chi_{\mathbb{Q}}(n\sqrt{2}) = 0$).

Ainsi, $\chi_{\mathbb{Q}}$ n'a pas de limite en $+\infty$.

Exercice 6.2.5.6 Montrer que $x \longmapsto \sin(x)$ n'admet pas de limite en $+\infty$.

Exercice 6.2.5.7 Montrer que f admet ℓ pour limite en a si et seulement si pour toute suite $(u_n)_{n\in\mathbb{N}} \in I^{\mathbb{N}}$, $(f(u_n))_{n\in\mathbb{N}}$ admet une limite (finie ou infinie).

Corollaire 6.2.5.8 *Soit $f : I \longrightarrow \mathbb{K}$ et $a \in I$. Alors f est continue en a si et seulement si pour toute suite $(u_n)_{n\in\mathbb{N}} \in I^{\mathbb{N}}$ convergeant vers a, $(f(u_n))$ converge vers $f(a)$.*

Preuve :

C'est une conséquence directe de la caractérisation séquentielle de la limite et de la définition de la continuité en a.

⊠

Remarques :

- *le dernier corollaire s'appelle la caractérisation séquentielle de la continuité (en un point) ;*
- *à nouveau c'est une caractérisation très importante que l'on utilise :*
  - ∗ *dans la pratique pour montrer qu'une fonction n'est pas continue en un point ;*
  - ∗ *dans la pratique (ou la théorie) lorsque l'on sait que la fonction est continue en un point.*
- *en particulier, cette propriété est toujours utilisée dans l'étude de suites définies par $u_{n+1} = f(u_n)$ lorsqu'on a déjà prouvé la convergence et qu'on souhaite déterminer la valeur de la limite.*

Exemple 6.2.5.9 Soit $(u_n)_{n\in\mathbb{N}}$ définie par $u_0 = 1$ et $\forall n \in \mathbb{N}$, $u_{n+1} = \sin(u_n)$. On a déjà vu [1] que (u_n) est décroissante et minorée donc converge. Soit $\ell = \lim\limits_{n\to+\infty} u_n$. Alors,

- d'une part, (u_{n+1}) est une suite extraite de $(u_n)_{n\in\mathbb{N}}$ donc elle converge vers ℓ ;
- d'autre part, la fonction sinus est continue en ℓ donc $\lim\limits_{n\to+\infty} \sin(u_n) = \sin(\ell)$.

Par unicité de la limite (par définition $(u_{n+1}) = (\sin(u_n))$), $\ell = \sin(\ell)$. Ensuite, on montre que l'unique solution possible est $\ell = 0$ en faisant par exemple une étude de fonction.

Exercice 6.2.5.10 Déterminer toutes les fonctions f, continues en 0 et vérifiant :

$$\forall x \in \mathbb{R} \ , \ f(\sin(x)) = f(x)$$

▶ Méthode :

L'idée principale dans ce type d'équation est d'itérer (c'est-à-dire répéter) la relation : ici

$$\forall n \in \mathbb{N} \ , \ f(\underbrace{\sin \circ \cdots \circ \sin}_{n \text{ fois}}(x)) = f(x)$$

puis de passer à la limite (sur le nombre d'itérations).

Voici quelques indications pour résoudre l'exercice : soit f continue en 0 et vérifiant la relation donnée. Soit $x \in \mathbb{R}$. On considère la suite $(u_n)_{n\in\mathbb{N}}$ définie par $u_0 = x$ et $\forall n \in \mathbb{N}$, $u_{n+1} = \sin(u_n)$.

1. Montrer que $(u_n)_{n\in\mathbb{N}}$ converge et déterminer sa limite.
2. Comparer pour $n \in \mathbb{N}$, $f(u_n)$ et $f(x)$.
3. En déduire que f est constante.

1. voir exercice 3.1.1.7.

6.2.6 Théorème de la limite monotone

Théorème 6.2.6.1 (Théorème de la limite monotone)

Soient $f : I \longrightarrow \mathbb{R}$ une application monotone sur I et $a \in \overline{I}$. Alors $\lim\limits_{x \to a^-} f(x)$ et $\lim\limits_{x \to a^+} f(x)$ existent (si $a \neq \inf I$ ou $a \neq \sup I$), c'est-à-dire f a une limite à gauche en a (si $a \neq \inf I$) et f a une limite à droite en a (si $a \neq \sup I$). Plus précisément,

- *si f est croissante, alors :*

$$\lim_{\substack{x \to a \\ x > a}} f(x) = \inf_{\substack{x \in I \\ x > a}} f(x) \qquad \text{et} \qquad \lim_{\substack{x \to a \\ x < a}} f(x) = \sup_{\substack{x \in I \\ x < a}} f(x)$$

  Par ailleurs, si $a \in \overset{\circ}{I}$, alors f admet des limites finies à droite et à gauche en a et :

$$\lim_{\substack{x \to a \\ x < a}} f(x) \leqslant f(a) \leqslant \lim_{\substack{x \to a \\ x > a}} f(x)$$

- *si f est décroissante, alors :*

$$\lim_{\substack{x \to a \\ x > a}} f(x) = \sup_{\substack{x \in I \\ x > a}} f(x) \qquad \text{et} \qquad \lim_{\substack{x \to a \\ x < a}} f(x) = \inf_{\substack{x \in I \\ x < a}} f(x)$$

  Par ailleurs, si $a \in \overset{\circ}{I}$, alors f admet des limites finies en a^+ et a^- et :

$$\lim_{\substack{x \to a \\ x < a}} f(x) \geqslant f(a) \geqslant \lim_{\substack{x \to a \\ x > a}} f(x)$$

En particulier, si $\alpha = \inf I$ et $\beta = \sup I$, alors f admet des limites (finies ou infinies) à droite en α et à gauche en β.

Corollaire 6.2.6.2 *Si f est croissante sur $[a, b[$ (avec $b \in \mathbb{R} \cup \{+\infty\}$), alors f admet une limite en b. De plus, cette limite est finie si et seulement si f est majorée.*

Corollaire 6.2.6.3 *Si f est croissante sur $]a, b]$ (avec $a \in \mathbb{R} \cup \{-\infty\}$) alors f admet une limite en a. De plus, cette limite est finie si et seulement si f est minorée.*

Preuve :

• Tout d'abord, quitte à remplacer f par $-f$, qui est également monotone, on peut supposer que f est décroissante. On obtient alors le résultat pour f croissante en utilisant les relations $\sup(-A) = -\inf A$ et $\inf(-A) = -\sup(A)$ (lorsque A est une partie non vide de $\mathbb{R}$).

• On commence par le cas $a \in \overset{\circ}{I}$.

∗ Montrons que f admet une limite finie à droite en a.
On considère l'ensemble $B = \{f(x)\ ,\ x \in I \cap]a, +\infty[\}$.

▷ B est une partie non vide de $\mathbb{R}$ car $a \in \overset{\circ}{I}$ donc $I \cap]a, +\infty[\neq \emptyset$.

▷ De plus, puisque f est décroissante sur I,

$$\forall x \in I \cap]a, +\infty[\ ,\ f(x) \leqslant f(a)$$

Par suite, B est majorée (par $f(a)$).

On en déduit donc que B admet une borne supérieure (dans $\mathbb{R}$) et on remarque aussi que $\sup B \leqslant f(a)$.

Montrons alors que $\lim\limits_{\substack{x \to a \\ x > a}} f(x) = \sup B$.
Soit $\varepsilon > 0$. D'après la caractérisation de la borne supérieure dans $\mathbb{R}$, il existe $b \in B$ tel que $\sup B - \varepsilon < b \leqslant \sup B$. Par définition de l'ensemble B, il existe $x_0 \in I \cap]a, +\infty[$ tel que $b = f(x_0)$. Alors, $]a, x_0[\subset I$ (car I est un intervalle) et :

$$\forall x \in]a, x_0[\ ,\ \sup B - \varepsilon < f(x_0) \leqslant f(x) \leqslant \sup B$$

En effet, si $x \in]a, x_0[$, alors :

▷ $f(x_0) \leqslant f(x)$ car f est décroissante sur I et $]a, x_0[\subset I$;

▷ $\sup B - \varepsilon < f(x_0)$ par définition de x_0 ;

▷ $x \in]a, x_0[\subset I \cap]a, +\infty[$, donc $f(x) \in B$ et $f(x) \leqslant \sup B$.

ce qui implique que : $\forall x \in]a, x_0[\ ,\ |f(x) - \sup B| \leqslant \varepsilon$.
Ceci prouve donc que f admet une limite finie à droite en a et $\lim\limits_{\substack{x \to a \\ x > a}} f(x) = \sup B$, c'est-à-dire :

$$\lim_{\substack{x \to a \\ x > a}} f(x) = \sup\{f(x)\ ,\ x \in I \cap]a, +\infty[\} = \sup_{\substack{x \in I \\ x > a}} f(x)$$

De plus, ayant remarqué que $\sup B \leqslant f(a)$, on a également :

$$\lim_{\substack{x \to a \\ x > a}} f(x) \leqslant f(a)$$

∗ Montrons à présent que f admet une limite finie à gauche en a.
De la même façon, on montre que :

▷ $C = \{f(x)\ ,\ x \in I \cap]-\infty, a[\}$ est non vide et minorée par $f(a)$ (car f est décroissante) donc C admet une borne inférieure (dans $\mathbb{R}$) et $f(a) \leqslant \inf C$;

▷ $\lim\limits_{x \to a^-} f(x) = \inf C$ en utilisant la caractérisation de la borne inférieure dans $\mathbb{R}$ (avec les "ε") et la définition formelle de la limite.

On conclut alors que : $\lim\limits_{\substack{x \to a \\ x > a}} f(x) \leqslant f(a) \leqslant \lim\limits_{\substack{x \to a \\ x < a}} f(x)$.

• Montrons à présent que f a une limite en $\beta = \sup I$ et que cette limite est finie si seulement si f est minorée sur I.

∗ On suppose que f est minorée.
Dans ce cas, l'ensemble $\{f(x)\ ,\ x \in I \cap]-\infty, \beta[\}$ est minoré (et non vide) donc il admet une borne inférieure (dans $\mathbb{R}$). Soit ℓ cette borne inférieure (qui appartient donc à $\mathbb{R}$). On recommence alors le même raisonnement que précédemment.
Soit $\varepsilon > 0$. D'après la caractérisation de la borne inférieure dans $\mathbb{R}$, il existe $x_0 \in I$ et $x_0 < \beta$ tel que $\ell \leqslant f(x_0) < \ell + \varepsilon$. Alors $]x_0, \beta[\subset I$ et :

$$\forall x \in]x_0, \beta[\ ,\ \ell - \varepsilon \leqslant \ell \leqslant f(x) \leqslant f(x_0) \leqslant \ell + \varepsilon$$

Ce qui prouve que $\lim\limits_{\substack{x \to \beta \\ x < \beta}} f(x) = \ell = \inf\limits_{\substack{x \in I \\ x < \beta}} f(x)$.

∗ On suppose que f n'est pas minorée sur I. Montrons que $\lim\limits_{x \to \beta^-} f(x) = -\infty$ (et $\beta \notin I$)
Tout d'abord, il est alors évident que $\beta = \sup I \notin I$ puisque sinon, $f(\beta)$ est un minorant de f. Ensuite, soit $M \in \mathbb{R}$. Puisque f n'est pas minorée sur I, M n'est pas un minorant de f sur I : il existe $x_1 \in I$ tel que $f(x_1) < M$. La fonction f étant décroissante, on en déduit que :

$$\forall x \in]x_1, \beta[\ ,\ f(x) \leqslant f(x_1) \leqslant M$$

Ceci prouve que $\lim\limits_{\substack{x \to \beta \\ x < \beta}} f(x) = -\infty$.

• On en déduit alors le résultat en α en appliquant le résultat précédent à $x \longmapsto -f(-x)$ sur l'intervalle $-I$.

⊠

6.3 Relations de comparaisons

6.3.1 Fonctions dominées et fonctions négligeables par rapport à une autre au voisinage d'un point

Les notions de o, O et équivalent ont déjà été introduites de façon pratique dans auparavant (définitions lorsque g ne s'annule pas à l'aide du quotient $\frac{f}{g}$).. Dans ce paragraphe, on va formaliser les définitions et les propriétés. L'utilisation pratique reste la même. On retiendra que :

- les définitions théoriques sont importantes lorsqu'on est confronté à un exercice théorique (l'expression de la fonction f n'est pas donnée) ;
- dans la pratique (c'est-à-dire lorsque l'expression de la fonction f est connue), on fait « comme d'habitude », c'est-à-dire comme ce qui a été appris dans les livres précédents.

Définition 6.3.1.1 Soient I un intervalle, $a \in \overline{I}$, f et g deux fonctions définies sur I. On dit que f est négligeable devant g au voisinage de a, et on note $f \underset{a}{=} o(g)$, si :

lorsque $a \in \mathbb{R}$: $\forall \varepsilon > 0\ ,\ \exists \alpha > 0\ ,\ \forall x \in I \cap]a-\alpha, a+\alpha[\ ,\ |f(x)| \leqslant \varepsilon |g(x)|$

lorsque $a = +\infty$: $\forall \varepsilon > 0\ ,\ \exists A \in \mathbb{R}\ ,\ \forall x \in I \cap]A, +\infty[\ ,\ |f(x)| \leqslant \varepsilon |g(x)|$

lorsque $a = -\infty$: $\forall \varepsilon > 0\ ,\ \exists A \in \mathbb{R}\ ,\ \forall x \in I \cap]-\infty, A[\ ,\ |f(x)| \leqslant \varepsilon |g(x)|$

Remarques :

- *bien entendu, on peut donner une définition unique qui englobe les trois cas à l'aide des voisinages :*

$$f \underset{a}{=} o(g) \iff \forall \varepsilon > 0\ ,\ \exists V \in \mathcal{V}(a)\ ,\ \forall x \in I \cap V\ ,\ |f(x)| \leqslant \varepsilon |g(x)|$$

- *cette définition s'applique aussi bien pour des fonctions à valeurs réelles que pour des fonctions à valeurs complexes.*

Proposition 6.3.1.2 *$f \underset{a}{=} o(g)$ si et seulement si il existe un voisinage V de a et une fonction h, définie sur $I \cap V$, tels que $f(x) = g(x)h(x)$ pour tout x dans $V \cap I$ et $\lim\limits_{x \to a} h(x) = 0$.*

Preuve :

• Montrons $\Longrightarrow$

On suppose que $f \underset{a}{=} o(g)$. Prenons pour commencer, $\varepsilon = 1 > 0$. Il existe alors un voisinage V_1 de a tel que :

$$(\star)\ \forall x \in I \cap V_1\ ,\ |f(x)| \leqslant |g(x)|$$

On définit alors la fonction h sur $I \cap V_1$ par :

$$h(x) = \begin{cases} \dfrac{f(x)}{g(x)} & \text{si } g(x) \neq 0 \\ \\ 0 & \text{si } g(x) = 0 \end{cases}$$

D'après $(\star)$, si $x \in I \cap V_1$ et $g(x) = 0$, alors $f(x) = 0$ également. Par suite, on a pour tout $x \in I \cap V_1$, $f(x) = h(x) \times g(x)$.
De plus, soit $\varepsilon > 0$. Il existe un voisinage V_ε de a tel que :

$$\forall x \in I \cap V_\varepsilon\ ,\ |f(x)| \leqslant \varepsilon |g(x)|$$

En posant $V = V_1 \cap V_\varepsilon$, V est un voisinage de a et pour tout $x \in I \cap V$:

- soit $g(x) = 0$, et dans ce cas, $|h(x)| = 0 \leqslant \varepsilon$;
- ou bien $g(x) \neq 0$, et dans ce cas, $|h(x)| = \left|\frac{f(x)}{g(x)}\right| \leqslant \varepsilon$.

Ainsi, dans les deux cas, $|h(x)| \leqslant \varepsilon$. Ce qui prouve que $\lim\limits_{x \to a} h(x) = 0$.

• La réciproque est évidente. En effet, s'il existe un voisinage V de a et une fonction h, définie sur $I \cap V$, tels que $f(x) = h(x) \times g(x)$ pour x dans $I \cap V$ et telle que $\lim\limits_{x \to a} h(x) = 0$, alors pour tout $\varepsilon > 0$, il existe un voisinage V_1 de a tel que : $\forall x \in I \cap V \cap V_1\ ,\ |h(x)| \leqslant \varepsilon$. Dans ce cas,

$$\forall x \in I \cap V \cap V_1\ ,\ |f(x)| = |g(x)| \times |h(x)| \leqslant \varepsilon |g(x)|$$

Ce qui prouve que $f \underset{a}{=} o(g)$.

⊠

Remarque : *attention, on ne peut pas toujours dire que f s'écrit $f = g \times h$ sur I tout entier car les relations de comparaison sont des comparaisons « locales », pas « globales ».*

Dans le cas particulier où la fonction g ne s'annule pas sur I, sauf peut-être au point a, on dispose d'une caractérisation plus simple qui est toujours utilisée dans la pratique (et qui correspond à la « définition » pratique que vous avez étudié ou appris avant.

Proposition 6.3.1.3 *Si g ne s'annule pas sur $I \setminus \{a\}$, alors on a deux cas :*

- *si $a \notin I$, alors : $f \underset{a}{=} o(g) \iff \lim\limits_{x\to a} \dfrac{f(x)}{g(x)} = 0$;*
- *si $a \in I$, alors : $f \underset{a}{=} o(g) \iff \left(f(a) = 0 \quad et \quad \lim\limits_{x\to a} \dfrac{f(x)}{g(x)} = 0\right)$.*

Preuve :

• Premier cas : $a \notin I$.

Dans ce cas, g ne s'annule pas sur I et on a alors :

$$\begin{aligned} f \underset{a}{=} o(g) &\iff \forall \varepsilon > 0\ ,\ \exists V \in \mathcal{V}_o(a)\ ,\ \forall x \in I \cap V\ ,\ |f(x)| \leqslant \varepsilon |g(x)| \\ &\iff \forall \varepsilon > 0\ ,\ \exists V \in \mathcal{V}_o(a)\ ,\ \forall x \in I \cap V\ ,\ \left|\frac{f(x)}{g(x)}\right| \leqslant \varepsilon \\ &\iff \lim_{x\to a} \frac{f(x)}{g(x)} = 0 \end{aligned}$$

• Deuxième cas : $a \in I$.

Dans ce cas, $f \underset{a}{=} o(g)$ est équivalent à :

$$\forall \varepsilon > 0\ ,\ \exists V \in \mathcal{V}_o(a)\ ,\ \forall x \in I \cap V\ ,\ |f(x)| \leqslant \varepsilon |g(x)|$$

soit encore :

$$\forall \varepsilon > 0\ ,\ \exists V \in \mathcal{V}_o(a)\ ,\ \forall x \in (I \cap V) \setminus \{a\}\ ,\ |f(x)| \leqslant \varepsilon |g(x)| \ \text{ et } \ |f(a)| \leqslant \varepsilon |g(a)|$$

c'est-à-dire :

$$\forall \varepsilon > 0\ ,\ \exists V \in \mathcal{V}_o(a)\ ,\ \forall x \in (I \cap V) \setminus \{a\}\ ,\ \left|\frac{f(x)}{g(x)}\right| \leqslant \varepsilon \quad \text{ et } \ f(a) = 0$$

Ce qui donne bien

$$\lim_{\substack{x\to a \\ x\neq a}} \frac{f(x)}{g(x)} = 0 \quad \text{et} \quad f(a) = 0$$

⊠

Remarques :

- *la distinction provient de l'ensemble de définition de $\frac{f}{g}$: si $a \in I$, cette fonction est définie sur $I \setminus \{a\}$ alors que si $a \notin I$, $\frac{f}{g}$ est définie sur I tout entier ;*

- *la proposition est vraie si l'on suppose seulement qu'il existe un voisinage V de a tel que g ne s'annule pas sur $V \setminus \{a\}$;*
- *dans la pratique, c'est ce critère qu'on utilise pour démontrer que $f \underset{a}{=} o(g)$. On utilise la définition formelle uniquement (ou presque) dans un cadre théorique ;*
- *on écrit aussi parfois $f \underset{x\to a}{=} o(g)$ et abusivement, on note $f(x) \underset{x\to a}{=} o(g(x))$;*
- *si on suppose que $a \in I$, que g ne s'annule pas sur $I \setminus \{a\}$ et que f et g continues en a, on a encore : $f \underset{a}{=} o(g) \iff \lim\limits_{x\to a} \dfrac{f(x)}{g(x)} = 0$.*

⚠ **Attention :** il faut garder à l'esprit que la notation $o(g)$ désigne une fonction. La relation $f(x) \underset{x\to 0}{=} x + o(x^2)$ est une égalité rigoureuse entre deux fonctions sur un certain voisinage de 0.

Exercice 6.3.1.4 Montrer que $\ln x \underset{x\to+\infty}{=} o(x)$ et $x^3 + 6x \underset{x\to 0}{=} o(\sqrt{x})$.

Définition 6.3.1.5 Soient I un intervalle, $a \in \overline{I}$, f et g deux fonctions définies sur I. On dit que f est dominée par g au voisinage de a, et on note $f \underset{a}{=} O(g)$ si :

$$\exists M > 0 \ , \ \exists V \in \mathcal{V}(a) \ , \ \forall x \in I \cap V \ , \ |f(x)| \leqslant M \, |g(x)|$$

Exercice 6.3.1.6 Reformuler cette définition en distinguant les cas où $a \in \mathbb{R}$, $a = +\infty$ et $a = -\infty$.

Proposition 6.3.1.7 *Avec les hypothèses précédentes, $f \underset{a}{=} O(g)$ si et seulement si il existe un voisinage V de a et une fonction h, définie sur $I \cap V$, tels que $f(x) = g(x)h(x)$ pour tout x dans $V \cap I$ et telle que h est bornée sur $V \cap I$.*

Preuve :

Il suffit de reprendre la démonstration dans le cas $f \underset{a}{=} o(g)$ et de l'adapter au cas $f \underset{a}{=} O(g)$. Les détails de la démonstration sont laissés en exercice !

⊠

Proposition 6.3.1.8 *Si g ne s'annule pas au voisinage de $a \in \overline{I}$ alors :*

$$f \underset{a}{=} O(g) \iff \frac{f}{g} \text{ est bornée au voisinage de } a$$

Par ailleurs, si $a \in I$ et g ne s'annule pas au voisinage de a, sauf en a, alors :

$$f \underset{a}{=} O(g) \iff \left(f(a) = 0 \quad et \quad \frac{f}{g} \text{ est bornée au voisinage de } a \right)$$

et si de plus on suppose que f et g sont continues en a, alors :

$$f \underset{a}{=} O(g) \iff \frac{f}{g} \text{ est bornée au voisinage de } a$$

Preuve :

• On commence par traiter le cas où g ne s'annule pas sur un certain voisinage V_0 de a. Dans ce cas, on a directement :

$$\begin{aligned} f \underset{a}{=} O(g) &\iff \exists M > 0, \exists V \in \mathcal{V}(a), \forall x \in I \cap V, |f(x)| \leqslant M\,|g(x)| \\ &\iff \exists M > 0, \exists V \in \mathcal{V}(a), \forall x \in I \cap V \cap V_0, |f(x)| \leqslant M\,|g(x)| \\ &\iff \exists M > 0, \exists V \in \mathcal{V}(a), \forall x \in I \cap (V \cap V_0), \left|\frac{f(x)}{g(x)}\right| \leqslant M \\ &\iff \frac{f}{g} \text{ est bornée au voisinage de } a \end{aligned}$$

• On suppose à présent qu'il existe un voisinage V_0 de a tel que g ne s'annule pas sur $V_0 \setminus \{a\}$ et $g(a) = 0$. Alors, comme précédemment, $f \underset{a}{=} O(g)$ est équivalent à l'existence de $M > 0$ et $V \in \mathcal{V}(a)$ tels que :

$$\forall x \in I \cap V \cap V_0 \ , \ |f(x)| \leqslant M\,|g(x)|$$

ce qui est ici équivalent à :

$$\forall x \in (I \setminus \{a\}) \cap V \cap V_0 \ , \ \left|\frac{f(x)}{g(x)}\right| \leqslant M \ \text{ et } \ |f(a)| \leqslant M|g(a)|$$

ou encore à

$$\frac{f}{g} \text{ est bornée au voisinage de } a \quad \text{et} \quad f(a) = 0$$

• Enfin, on suppose que $a \in I$ et que f et g sont continues en a et qu'il existe un voisinage V_0 de a tel que g ne s'annule pas sur $V_0 \setminus \{a\}$ et $g(a) = 0$. D'après ce qui précède :

$$f \underset{a}{=} O(g) \iff \frac{f}{g} \text{ est bornée au voisinage de } a \quad \text{et} \quad f(a) = 0$$
$$\implies \frac{f}{g} \text{ est bornée au voisinage de } a$$

Il s'agit donc d'établir la réciproque, c'est-à-dire de montrer que si $\frac{f}{g}$ est bornée au voisinage de a (et avec les hypothèses données ci-dessus), alors nécessairement, $f(a) = 0$.
Pour cela, il suffit de constater que si $\frac{f}{g}$ est bornée au voisinage de a, il existe un voisinage V de a et un réel $M \geqslant 0$ tels que :

$$\forall x \in (I \setminus \{a\}) \cap V \ , \ \left|\frac{f(x)}{g(x)}\right| \leqslant M$$

Il s'ensuit que : $\forall x \in (I \cap V) \setminus \{a\}$, $|f(x)| \leqslant M\,|g(x)|$. Or, on a supposé que f et g sont continues en a. Par suite,

$$|f(a)| = \lim_{\substack{x \to a \\ x \neq a}} |f(x)| \leqslant M \times \lim_{\substack{x \to a \\ x \neq a}} |g(x)| \ \leqslant M \times |g(a)| = 0$$

D'où l'on déduit que $f(a) = 0$. ⊠

Exemple 6.3.1.9 Montrons que $x^2 \sin(\frac{1}{x}) \underset{x \to 0}{=} o(x)$ ou encore que $x^2 \sin(\frac{1}{x}) \underset{x \to 0}{=} O(x^2)$.

Dans cet exemple, $0 \notin I$ (puisque $f : x \longmapsto x^2 \sin(\frac{1}{x})$ n'est pas définie en 0) et il est clair que $g(x) = x$ ne s'annule pas sur $\mathbb{R}^\star$. Par suite, on peut directement écrire que :

$$\lim_{x \to 0} \frac{x^2 \sin(\frac{1}{x})}{x} = 0 \quad \text{(théorème des gendarmes)}$$

c'est-à-dire que $x^2 \sin(\frac{1}{x}) \underset{x \to 0}{=} o(x)$.
En particulier, on en déduit que : $\lim\limits_{\substack{x \to 0 \\ x \neq 0}} \left(x^2 \sin(\frac{1}{x})\right) = 0$, c'est-à-dire que l'on peut prolonger la fonction f par continuité en 0 en posant $f(0) = 0$. On reverra un peu plus loin cette notion de prolongement par continuité.

Par ailleurs, $x \longmapsto \sin(\frac{1}{x})$ étant bornée au voisinage de 0, $x^2 \sin(\frac{1}{x}) \underset{x \to 0}{=} O(x^2)$.

Exemple 6.3.1.10 On a $\dfrac{1}{1+x^2} \underset{x \to +\infty}{=} o(1)$ et aussi $\dfrac{1}{1+x^2} \underset{x \to 0}{=} O(1)$.

Exemple 6.3.1.11 On considère les fonctions f et g définies respectivement par :

$$\forall x \in \mathbb{R}\ ,\ f(x) = x^2 \sin(x) \quad \text{et} \quad \forall x \in \mathbb{R}\ ,\ g(x) = (5x^2 + x + 1)\sin(x)$$

On veut montrer que $g \underset{+\infty}{=} O(f)$. Dans cet exemple, il n'y a pas de voisinage de $+\infty$ sur lequel la fonction f ne s'annule pas. On ne peut donc pas utiliser le critère pratique ($\frac{g}{f}$). En revanche, on peut dire qu'il existe $A > 0$ tel que :

$$\forall x \geqslant A\ ,\ |5x^2 + x + 1| \leqslant 7x^2$$

Par suite,

$$\forall x \geqslant A\ ,\ |g(x)| = |5x^2 + x + 1| \times |\sin(x)| \leqslant 7|x^2| \times |\sin(x)|$$

c'est-à-dire que pour tout $x \geqslant A$, $|g(x)| \leqslant 7|f(x)|$. Ce qui prouve que $g \underset{+\infty}{=} O(f)$.

Exemple 6.3.1.12 Soient $f = \delta_0$ (c'est-à-dire $f = \chi_{\{0\}}$) et $g : x \longmapsto x$. Bien que $\lim\limits_{\substack{x\to 0\\ x>0}} \dfrac{f(x)}{g(x)} = 0 = \lim\limits_{\substack{x\to 0\\ x<0}} \dfrac{f(x)}{g(x)}$, f n'est pas un petit o de g !

Remarque : *n'oubliez jamais que les o et les O désignent des fonctions vérifiant une certaine propriété. On peut donc avoir $f = o(h)$ et $g = o(h)$ sans avoir $f = g$!! Par exemple, pour tout entier n, $x^n \underset{x\to+\infty}{=} o(e^x)$ (par croissances comparées).*

Dans le même esprit, si $g \underset{a}{=} o(f) - o(f)$ (ou $h \underset{a}{=} O(f) - O(f)$), alors g (ou h) n'est pas nécessairement égale à 0 ! Cette égalité se traduit par le fait qu'il existe deux fonctions φ_1 et φ_2, définies au voisinage V de a, telles que :

- $\forall x \in V\ ,\ g(x) = \varphi_1(x) - \varphi_2(x)$;
- *les fonctions φ_1 et φ_2 sont négligeables devant f.*

Proposition 6.3.1.13 *Soit f une fonction définie au voisinage de a. Alors :*

$$f \underset{a}{=} o(1) \iff \lim_{x\to a} f(x) = 0 \quad \textit{et} \quad f \underset{a}{=} O(1) \iff \textit{f est bornée au voisinage de } a$$

Preuve :

C'est clair !

⊠

La proposition suivante donne des règles de « bon sens » concernant les o et O. Les démonstrations sont laissées en exercice et sont évidentes.

Proposition 6.3.1.14 *Les relations o et O vérifient les propriétés suivantes :*

1. *si* $f \underset{a}{=} o(g)$, *alors* $f = O(g)$;
2. *si* $f \underset{a}{=} o(\varphi)$ *et* $g \underset{a}{=} o(\varphi)$, *alors* $\forall \lambda \in \mathbb{K}$, $\lambda \cdot f + g \underset{a}{=} o(\varphi)$;
3. *si* $f \underset{a}{=} O(\varphi)$ *et* $g \underset{a}{=} O(\varphi)$, *alors* $\forall \lambda \in \mathbb{K}$, $\lambda \cdot f + g \underset{a}{=} O(\varphi)$;
4. *si* $f \underset{a}{=} o(\varphi)$ *et* $g \underset{a}{=} o(\psi)$, *alors* $fg \underset{a}{=} o(\varphi\psi)$;
5. *si* $f \underset{a}{=} o(\varphi)$ *et* $g \underset{a}{=} O(\psi)$, *alors* $fg \underset{a}{=} o(\varphi\psi)$;
6. *si* $f \underset{a}{=} O(\varphi)$ *et* $g \underset{a}{=} O(\psi)$, *alors* $fg \underset{a}{=} O(\varphi\psi)$;
7. *si* $f \underset{a}{=} O(\varphi)$ *et* $\varphi \underset{a}{=} o(\psi)$, *alors* $f \underset{a}{=} o(\psi)$.

Remarque : *il faut retenir qu'on peut manipuler les o ou O comme d'habitude avec le « bon sens » : dominée par du négligeable est négligeable.*

Exemple 6.3.1.15 Si on utilise les théorèmes de croissances comparées, on peut dire que :

$$\ln(x) \underset{x\to+\infty}{=} o(x) \quad \text{et} \quad x \underset{x\to+\infty}{=} o(e^x)$$

On en déduit donc que $\ln(x) \underset{x\to+\infty}{=} o(e^x)$.

Exemple 6.3.1.16 Soit $f(x) = (10x^2 + 13x - 1)\arctan(x)$. On a alors :

$$(10x^2 + 13x - 1) \underset{x\to+\infty}{=} O(x^2) \quad \text{et} \quad \arctan(x) \underset{x\to+\infty}{=} O(1)$$

On en déduit donc que : $f(x) \underset{x\to+\infty}{=} O(x^2 \times 1)$, c'est-à-dire $f(x) \underset{x\to+\infty}{=} O(x^2)$.

6.3.2 Comparaison des fonctions usuelles

Les résultats suivants découlent des théorèmes de croissances comparées :

Théorème 6.3.2.1 *On a les relations de comparaisons suivantes au voisinage de* $+\infty$ *:*

- *Pour tout* $\alpha > 0$ *et tout* $\beta \in \mathbb{R}$, $(\ln x)^\beta \underset{x\to+\infty}{=} o(x^\alpha)$
- *Si* $\alpha < \beta$, $(x^\alpha) \underset{x\to+\infty}{=} o(x^\beta)$
- *Pour tout* $\alpha > 0$ *et tout* $\beta \in \mathbb{R}$, $x^\beta \underset{x\to+\infty}{=} o(e^{\alpha x})$

Preuve :

Ces propriétés ont probablement été prouvées avant. On rappelle ici une méthode de démonstration :

- on commence par établir que $\ln(x) \leqslant 1+x$ pour $x > -1$ (étude de fonction par exemple) ;
- on en déduit que $\lim\limits_{x\to+\infty} \dfrac{\ln(x)}{x^2} = 0$ (théorème des gendarmes) ;
- ensuite, pour $\alpha > 0$, $\frac{|\ln(x)|}{x^\alpha} = \frac{2}{\alpha}\frac{|\ln x^{\frac{\alpha}{2}}|}{(x^{\frac{\alpha}{2}})^2}$ montre que $\lim\limits_{x\to+\infty} \dfrac{\ln x}{x^\alpha} = 0$.

La propriété sur les exponentielles se déduit de celles pour ln.

⊠

6.3.3 Fonctions équivalentes en un point

Définition 6.3.3.1 Soient f et g deux fonctions définies sur I et $a \in \overline{I}$. On dit que f est équivalente à g au voisinage de a, et on note $f \underset{a}{\sim} g$, si $f - g \underset{a}{=} o(g)$.

Proposition 6.3.3.2 *Soient f et g deux fonctions définies sur I et $a \in \overline{I}$. Alors $f \underset{a}{\sim} g$ si et seulement si il existe un voisinage V de a et une fonction u définie sur $I \cap V$ tels que :*

$$\forall x \in I \cap V \ , \ f(x) = u(x)g(x) \quad \text{et} \quad \lim_{x\to a} u(x) = 1$$

Preuve :

En effet, d'après la caractérisation des o, $f \underset{a}{\sim} g$ si et seulement s'il existe $V \in \mathcal{V}(a)$ et $h \in \mathcal{F}(V \cap I, \mathbb{K})$ tels que :

$$\forall x \in I \cap V \ , \ f(x) - g(x) = h(x)g(x) \ \text{ et } \ \lim_{x\to a} h(x) = 0$$

ce qui est équivalent à

$$\forall x \in I \cap V \ , \ f(x) = (1+h(x))g(x) \ \text{ et } \ \lim_{x\to a} h(x) = 0$$

ou encore à l'existence de $V \in \mathcal{V}(a)$ et $u \in \mathcal{F}(V \cap I, \mathbb{K})$ tels que :

$$\forall x \in I \cap V \ , \ f(x) = u(x)g(x) \ \text{ et } \ \lim_{x\to a} u(x) = 1$$

⊠

Corollaire 6.3.3.3 *La relation* $\underset{a}{\sim}$ *est une relation d'équivalence sur l'ensemble des fonctions définies sur* I *(on rappelle que* $a \in \overline{I}$*).*

Preuve :

Montrons que $\underset{a}{\sim}$ est réflexive, symétrique et transitive.

• Montrons la réflexivité.
Pour toute fonction f définie sur I, $f - f = 0$ donc $f - f \underset{a}{=} o(f)$. Par suite, $f \underset{a}{\sim} f$ et la relation est bien réflexive.

• Montons la symétrie.
Soient f et g définies sur I telles que $f \underset{a}{\sim} g$. D'après la proposition précédente, il existe un voisinage V de a et $u \in \mathcal{F}(V \cap I, \mathbb{K})$ tels que :

$$\forall x \in I \cap V \ , \ f(x) = u(x)g(x) \quad \text{et} \quad \lim_{x \to a} u(x) = 1$$

Par ailleurs, puisque $\lim\limits_{x \to a} u(x) = 1 \neq 0$, il existe un voisinage V' de a tel que, pour tout $x \in I \cap V \cap V'$, $u(x) \neq 0$. Alors $U = V \cap V' \in \mathcal{V}(a)$ et :

$$\forall x \in I \cap U \ , \ g(x) = \frac{1}{u(x)} \times f(x) \quad \text{avec} \quad \lim_{x \to a} \frac{1}{u(x)} = 1$$

Par conséquent, toujours d'après la proposition précédente, $g \underset{a}{\sim} f$. Ce qui prouve que $\underset{a}{\sim}$ est symétrique.

• Montrons enfin que la relation est transitive.
Soient f, g, h trois fonctions définies sur I telles que : $f \underset{a}{\sim} g$ et $g \underset{a}{\sim} h$. Il existe deux voisinages V et V' de a et deux fonctions u et v, définies sur $V \cap I$ et $V' \cap I$ respectivement, tels que :

$$\forall x \in I \cap V \ , \ f(x) = u(x)g(x) \quad \text{et} \quad \lim_{x \to a} u(x) = 1$$

$$\forall x \in I \cap V' \ , \ g(x) = v(x)h(x) \quad \text{et} \quad \lim_{x \to a} v(x) = 1$$

Soient $U = V \cap V'$ et w définie sur $U \cap I$ par : $w(x) = u(x)v(x)$. Alors :

$$\forall x \in I \cap U \ , \ f(x) = u(x)g(x) = u(x)v(x)h(x) = w(x)h(x)$$

et par arithmétique des limites, $\lim\limits_{x \to a} w(x) = 1$. Par suite, $f \underset{a}{\sim} h$, prouvant ainsi la transitivité. ⊠

Exercice 6.3.3.4 Montrer que $\underset{a}{\sim}$ est symétrique à partir de la définition formelle.

Remarques :

- *en particulier, $f \sim g$ implique que $f = O(g)$ et $g = O(f)$, la réciproque étant fausse (par exemple $f : x \longmapsto x$ et $g : x \longmapsto x(2+\cos(x))$ au voisinage de $+\infty$) ;*
- *ayant prouvé que $\underset{a}{\sim}$ est symétrique, on dit souvent que f et g sont équivalentes en a au lieu de f est équivalente à g en a.*

Comme pour les O ou o, on dispose d'une caractérisation « simple » à l'aide du quotient $\frac{f}{g}$ (lorsque celui-ci est bien défini). Enfin, notez bien la dernière conclusion qui est très importante et qui permet (dans le cas des fonctions à valeurs réelles) de comparer le signe.

Proposition 6.3.3.5 *Soient f et g deux fonctions définies au voisinage de a telles que $f \underset{a}{\sim} g$.*

(i) Si g ne s'annule pas au voisinage de a, alors :

$$f \underset{a}{\sim} g \iff \lim_{x\to a} \frac{f(x)}{g(x)} = 1$$

(ii) Si $a \in I$ et g ne s'annule pas au voisinage de a, sauf en a, alors :

$$f \underset{a}{\sim} g \iff \left(f(a) = g(a) \quad et \quad \lim_{\substack{x\to a \\ x\neq a}} \frac{f(x)}{g(x)} = 1 \right)$$

(iii) Si $a \in I$, g ne s'annule pas au voisinage de a, sauf en a, et si f et g sont continues en a, alors :

$$f \underset{a}{\sim} g \iff \lim_{\substack{x\to a \\ x\neq a}} \frac{f(x)}{g(x)} = 1$$

(iv) Si f et g sont à valeurs réelles, alors f et g sont de même signe (strictement) au voisinage de a. Autrement dit, il existe un voisinage V de a tel que, pour tout $x \in I \cap V$:

- *$f(x) = 0 \iff g(x) = 0$;*
- *$f(x) > 0 \iff g(x) > 0$.*

Remarque importante : *prenez l'habitude de toujours vérifier que les équivalents obtenus ont bien le même signe. Le « signe » en mathématiques est l'analogue de « l'homogénéité » en physique (et permet donc d'éliminer une réponse manifestement fausse).*

Preuve :

• Les propriétés (i) et (ii) ont déjà été prouvées (conséquence de la proposition 6.3.3.2 par exemple).

• Pour la propriété (iii), il suffit d'appliquer la propriété similaire avec les o aux fonctions $f_1 = f - g$ et $g_1 = g$.

• Enfin, montrons (iv).

Par hypothèse, $f \underset{a}{\sim} g$. Il existe donc un voisinage U de a et une fonction u définie sur $U \cap I$ tels que :

$$\forall x \in I \cap U \ , \ f(x) = u(x)g(x) \quad \text{et} \quad \lim_{x \to a} u(x) = 1$$

Par définition de la limite, il existe un voisinage U' de a tel que :

$$\forall x \in I \cap U \cap U' \ , \ |u(x) - 1| \leqslant \frac{1}{2}$$

Alors, pour tout $x \in I \cap U \cap U'$, $\frac{1}{2} \leqslant u(x) \leqslant \frac{3}{2}$. Il s'ensuit que $u > 0$ sur $I \cap U \cap U'$.
En posant $V = U \cap U'$, V est un voisinage de a et pour tout $x \in V \cap I$,

$$f(x) = u(x)g(x)$$

avec $u > 0$. D'où l'on déduit immédiatement que f et g sont de même signe strictement au voisinage de a.

⊠

Remarques :

- *dans un cadre théorique, en particulier lorsqu'on ne peut prouver que f (ou g) ne s'annule pas ailleurs qu'en a, il faut utiliser la définition de départ, c'est-à-dire $f - g \underset{a}{=} o(g)$ avec la définition formelle par les « ε » ;*
- *en fonction de la situation, c'est-à-dire s'il est facile de justifier que f (ou g) ne s'annule pas ailleurs qu'en a, et/ou s'il est plus facile d'estimer le quotient $\frac{f}{g}$ ou la différence $f - g$, on utilise l'une ou l'autre des différentes caractérisations ;*
- *un cas particulier important : si $\ell \neq 0$, alors $f \underset{a}{\sim} \ell$ équivaut à $\lim\limits_{x \to a} f(x) = \ell$;*
- *enfin, $f \underset{a}{\sim} 0$ si et seulement si f est identiquement nulle au voisinage de a.*

Exercice 6.3.3.6 Donner un équivalent de $e^{3x} - 4e^{x^2} + 7\ln x$ en $+\infty$, en 0 et enfin, en 1.

La proposition suivante découle directement de la caractérisation de l'équivalence (avec « l'existence d'une fonction u ») : la preuve est laissée en exercice.

Proposition 6.3.3.7 *La relation $\sim$ est compatible avec la multiplication et la division, c'est-à-dire :*

$$f \underset{a}{\sim} g \quad et \quad \phi \underset{a}{\sim} \psi \Longrightarrow \left(f\phi \underset{a}{\sim} g\psi \quad et \quad \frac{1}{f} \underset{a}{\sim} \frac{1}{g} \right)$$

La dernière implication étant valable lorsque f (et donc g) ne s'annule pas au voisinage de a, sauf peut-être en a.

⚠ **Attention :** on ne peut pas composer les équivalents ni les additionner directement. Par exemple,

- $x \underset{+\infty}{\sim} x+1$, mais $e^x \underset{+\infty}{\not\sim} e^{x+1}$;
- de même, $x+1 \sim x$ et $-x+2 \sim -x$ mais $3 \not\sim 0$!!

Pour contourner ce problème (et surtout éviter les erreurs), lorsque l'on souhaite « composer », on écrira toujours l'équivalence par une égalité avec des o.

6.3.4 Équivalents usuels

Proposition 6.3.4.1 *On a les équivalents usuels suivants (avec $\alpha \in \mathbb{R}$ une constante) :*

$\sin x \underset{0}{\sim} x$	$1-\cos(x) \underset{0}{\sim} \frac{1}{2}x^2$	$\tan x \underset{0}{\sim} x$	$\ln(1+x) \underset{0}{\sim} x$
$\mathrm{sh}\,(x) \underset{0}{\sim} x$	$\mathrm{ch}\,(x)-1 \underset{0}{\sim} \frac{x^2}{2}$	$\mathrm{th}\,(x) \underset{0}{\sim} x$	$(1+x)^\alpha - 1 \underset{0}{\sim} \alpha x$
	$\arcsin(x) \underset{0}{\sim} x$	$\arctan x \underset{0}{\sim} x$	$\arccos(x) \underset{1}{\sim} \sqrt{2(1-x)}$
$e^x - 1 \underset{0}{\sim} x$	$\mathrm{Argth}\,(x) \underset{0}{\sim} x$	$\mathrm{Argsh}\,(x) \underset{0}{\sim} x$	$\mathrm{Argch}\,(x) \underset{1}{\sim} \sqrt{2(x-1)}$

Preuve :

• La majeure partie de ces équivalents usuels a déjà été vu (si vous avez étudié les fonctions usuelles). La démonstration repose essentiellement sur la propriété suivante : si f est dérivable en 0 et $f'(0) \neq 0$, alors $(f(x) - f(0)) \underset{x\to 0}{\sim} f'(0)x$.

• Pour l'équivalent de cos (et de ch), il s'agit d'une conséquence de la relation $1 - \cos(x) = 2\sin^2(\frac{x}{2})$ et de l'équivalent de sin en 0 (et pour ch, de la relation $\mathrm{ch}\,(x) - 1 = 2\mathrm{sh}^2(\frac{x}{2})$ et de l'équivalent de sh en 0).

• Enfin les seuls équivalents qui n'ont pas été démontrés par ces méthodes sont les équivalents de arccos et Argch. Les démonstrations de ces deux propriétés sont semblables : on prouve donc la relation pour arccos (celle pour Argch est laissée en exercice).
On sait que $\lim\limits_{\substack{x\to 1\\ x<1}} \arccos(x) = 0$. Par composition de limites,

$$\sin(\arccos(x)) \underset{x\to 1}{\sim} \arccos(x)$$

Or, pour $x \in [0,1]$, $\arccos(x) \in [0, \frac{\pi}{2}]$ donc $\sin(\arccos(x)) \geqslant 0$ et on a :

$$\begin{aligned}\sin(\arccos(x)) &= |\sin(\arccos(x))| \\ &= \sqrt{1 - \cos^2(\arccos(x))} \\ &= \sqrt{1-x^2} \\ &= \sqrt{1+x} \times \sqrt{1-x}\end{aligned}$$

Enfin, puisque $\lim\limits_{\substack{x\to 1\\ x<1}} \sqrt{1+x} = \sqrt{2} \neq 0$, $\sqrt{1+x} \times \sqrt{1-x} \underset{x\to 1}{\sim} \sqrt{2}\sqrt{1-x}$.
D'où l'on déduit que :

$$\arccos(x) \underset{x\to 1}{\sim} \sin(\arccos(x)) \underset{x\to 1}{\sim} \sqrt{2}\sqrt{1-x}$$

⊠

Proposition 6.3.4.2 *Soient f et g deux fonctions définies sur I et $a \in \overline{I}$. On suppose que $f \underset{a}{\sim} g$.*

(i) f admet une limite (finie ou non) en a si et seulement si g admet une limite (finie ou non) en a. De plus, lorsqu'elles existent : $\lim\limits_{x\to a} f(x) = \lim\limits_{x\to a} g(x)$.

(ii) Si $f > 0$ au voisinage de a, sauf peut-être en a, alors pour tout réel α : $f^\alpha \underset{a}{\sim} g^\alpha$.

Preuve :

• Montrons (i).

Puisque $f \underset{a}{\sim} g$, il existe un voisinage V de a et $u \in \mathcal{F}(I \cap V, \mathbb{K})$ tels que :

$$\forall x \in I \cap V \ , \ f(x) = u(x)g(x) \quad \text{et} \ \lim_{x \to a} u(x) = 1$$

Supposons que g admette une limite ℓ (éventuellement infinie si $\mathbb{K} = \mathbb{R}$) en a. Alors par arithmétique des limites, f admet également ℓ pour limite en a.
Les rôles de f et g étant symétriques, on obtient la propriété (i).

• Montrons (ii).

On peut noter que l'hypothèse $f > 0$ au voisinage de a, sauf peut-être en a, permet de justifier que f^α est bien définie au voisinage de a, sauf peut-être en a (on rappelle que pour $t > 0$, $t^\alpha = e^{\alpha \ln(t)}$).
Par ailleurs, puisque $f \underset{a}{\sim} g$, g est elle aussi strictement positive au voisinage de a, sauf peut-être en a, et la fonction g^α est donc elle aussi bien définie au voisinage de a, sauf peut-être en a.
Enfin, puisque $f \underset{a}{\sim} g$, il existe un voisinage V_1 de a et $u \in \mathcal{F}(I \cap V_1, \mathbb{K})$ tels que :

$$\forall x \in I \cap V_1 \ , \ f(x) = u(x)g(x) \quad \text{et} \ \lim_{x \to a} u(x) = 1$$

Il existe aussi un voisinage V_2 de a tel que : $\forall x \in I \cap V_2 \setminus \{a\} \ , \ f(x) > 0$.
Il existe également un voisinage V_3 de a tel que : $\forall x \in I \cap V_3 \ , \ u(x) > 0$.
Posons $V = V_1 \cap V_2 \cap V_3$. Alors, V est un voisinage de a et :

$$\forall x \in (I \cap V) \setminus \{a\} \ , \ f^\alpha(x) = u^\alpha(x) \times g^\alpha(x)$$

Et $\lim\limits_{x \to a} u^\alpha(x) = 1$. On remarque alors que :

- si $f(a) = 0$ (et donc $g(a) = 0$), a n'appartient pas à l'ensemble de définition de f^α et on conclut donc que $f^\alpha \underset{a}{\sim} g^\alpha$;
- si $f(a) \neq 0$, alors $g(a) = f(a)$ et par suite $f^\alpha(a) = g^\alpha(a)$. Cette égalité et la relation ci-dessus montrent que $f^\alpha \underset{a}{\sim} g^\alpha$.

⊠

⚠ **Attention :** dans cette proposition, α est une constante ! Lorsque α est une fonction, c'est une composition d'équivalents qui n'est donc pas autorisée. Par exemple, si on choisit $f : x \longmapsto 1 + \frac{1}{x}$ et $g : x \longmapsto 1$, alors :

$$f \underset{+\infty}{\sim} g \quad \text{mais} \ f(x)^x \underset{x \to +\infty}{\sim} e \neq 1 \underset{x \to +\infty}{\sim} g(x)^x$$

⚠ **Attention :** la composition d'équivalents est strictement interdite ! Dans la proposition précédente, on a en fait utilisé une composition de limite. À titre d'exemple, rappelons un calcul d'équivalent simple correct et incorrect :

INCORRECT	CORRECT
$\ln(\cos(x)) \underset{x\to 0}{\sim} \ln(1-\frac{x^2}{2}) \underset{x\to 0}{\sim} -\frac{1}{2}x^2$	$\ln(\cos(x)) \underset{x\to 0}{\sim} \cos(x)-1 \underset{x\to 0}{\sim} -\frac{1}{2}x^2$
La première ligne est une composition d'équivalent, qui n'est pas autorisée (même si elle donne le bon résultat). On a implicitement écrit : $\cos(x) \underset{x\to 0}{\sim} 1-\frac{x^2}{2}$ **donc** $\ln(\cos(x)) \underset{x\to 0}{\sim} \ln(1-\frac{x^2}{2})$. Notez également au passage que l'équivalent : $\cos(x) \underset{x\to 0}{\sim} 1-\frac{x^2}{2}$ est parfaitement illogique ! $\cos(x) \underset{x\to 0}{\sim} 1$ est l'équivalent simple en 0. Le terme suivant n'est pas significatif. On pourrait aussi bien écrire : $\cos(x) \underset{x\to 0}{\sim} 1+x^{22032012}$	Cette fois, ce n'est pas une composition d'équivalents mais une composition avec une limite. Autrement dit, $\lim_{x\to 0}\cos(x)=1$ et $\ln(u) \underset{u\to 1}{\sim} (u-1)$ donc : $\ln(\cos(x)) \underset{x\to 0}{\sim} \cos(x)-1$. Notez qu'on peut également contourner le problème en utilisant les o. En notant $u : x \longmapsto \ln(\cos(x))$, on a : $u(x) \underset{x\to 0}{=} \ln(1-\frac{x^2}{2}+o(x^2)) \underset{x\to 0}{=} -\frac{x^2}{2}+o(x^2)+o(-\frac{x^2}{2}+o(x^2)) \underset{x\to 0}{=} -\frac{x^2}{2}+o(x^2)$

Exercice 6.3.4.3 Calculer les limites suivantes :

1. $\lim_{x\to 0} \dfrac{\ln(1+2\tan^2 x)}{\arcsin x}$
2. $\lim_{\substack{x\to 0\\ x>0}} \dfrac{\sqrt{\cos(2x)}-\operatorname{ch}(x)}{x^x-1}$
3. Pour $a>b>0$, $\lim_{x\to 0} \dfrac{a^x-b^x}{x^a-x^b}$

6.4 Continuité globale

6.4.1 Définition et premières propriétés

Définition 6.4.1.1 On dit qu'une fonction f est continue sur un intervalle I si elle est continue en tout point $a \in I$.

Exemple 6.4.1.2 La fonction exponentielle est continue sur $\mathbb{R}$.

Exemple 6.4.1.3 La fonction partie entière n'est pas continue sur $\mathbb{R}$: elle est continue en tout point de $\mathbb{R} \setminus \mathbb{Z}$ (on dira alors qu'elle est continue sur $\mathbb{R} \setminus \mathbb{Z}$, même si $\mathbb{R} \setminus \mathbb{Z}$ n'est pas un intervalle) et discontinue en tout point de $\mathbb{Z}$.

Exercice 6.4.1.4 Soit f l'application de $\mathbb{R}$ dans $\mathbb{R}$, qui à un réel x associe le nombre réel obtenu en échangeant les deux premières décimales du développement propre de x. Par exemple, $f(1,234) = 1,324$.
La fonction f est-elle continue sur $\mathbb{R}$? Déterminer l'ensemble des points où f est continue.

Proposition 6.4.1.5 *L'ensemble des fonctions continues sur I à valeurs dans $\mathbb{K}$ est noté $\mathcal{C}^0(I,\mathbb{K})$.*

- *$\mathcal{C}^0(I,\mathbb{K})$ est une sous-algèbre de $\mathcal{F}(I,\mathbb{K})$, c'est-à-dire un sous-anneau et un sous-espace vectoriel de $\mathcal{F}(I,\mathbb{K})$;*
- *si $f \in \mathcal{C}^0(I,\mathbb{K})$ et si f ne s'annule pas sur I, alors $\dfrac{1}{f}$ est continue sur I.*

Preuve :

| Ceci découle directement des propriétés des limites en un point.

⊠

Proposition 6.4.1.6 *Soient $f, g \in \mathcal{C}^0(I,\mathbb{K})$.*

(i) Alors $|f| \in \mathcal{C}^0(I,\mathbb{R})$;

(ii) si de plus $\mathbb{K} = \mathbb{R}$, alors $\sup(f,g)$ et $\inf(f,g)$ sont aussi continues sur I.

Preuve :

• Montrons (i).
Soit $a \in I$: montrons que $|f|$ est continue en a. Pour tout $x \in I$, on a :

$$\big||f(x)| - |f(a)|\big| \leqslant |f(x) - f(a)|$$

Or, $\lim\limits_{x\to a} f(x) = f(a)$ (puisque f est continue sur I), soit encore : $\lim\limits_{x\to a} |f(x) - f(a)| = 0$. Par suite, d'après le théorème des gendarmes, $\lim\limits_{x\to a} |f(x)| = |f(a)|$, c'est-à-dire $|f|$ est continue en a.

• Montrons (ii).
Pour cela, il suffit de remarquer que :

$$\sup(f,g) = \frac{1}{2}\left(f + g + |f - g|\right) \quad \text{et} \quad \inf(f,g) = \frac{1}{2}\left(f + g - |f - g|\right)$$

En utilisant (i) et le fait que l'ensemble des fonctions continues sur I est un espace vectoriel, on déduit immédiatement que $\sup(f,g)$ et $\inf(f,g)$ sont continues sur I.

⊠

Exercice 6.4.1.7 Faire la démonstration à la main (c'est-à-dire en utilisant la définition formelle de la limite) en traitant les cas $f(a) = g(a)$ puis $f(a) > g(a)$ (montrer qu'alors, au voisinage de a, $\sup(f,g) = f$).

⚠ **Attention :** la réciproque de la propriété (i) est fausse ! Autrement dit,

$$f \in \mathcal{C}^0(I,\mathbb{K}) \Longrightarrow |f| \in \mathcal{C}^0(I,\mathbb{K}) \quad \text{mais} \quad |f| \in \mathcal{C}^0(I,\mathbb{K}) \not\Longrightarrow f \in \mathcal{C}^0(I,\mathbb{K})$$

Par exemple, $f : x \longmapsto (-1)^{E(x)}$ n'est pas continue sur $\mathbb{R}$ (elle est discontinue en tout point entier relatif) alors que $|f| = 1$ est constante et donc continue sur $\mathbb{R}$.

Proposition 6.4.1.8 *On suppose ici que $\mathbb{K} = \mathbb{C}$. Soit $f \in \mathcal{F}(I,\mathbb{C})$. Alors les propriétés suivantes sont équivalentes :*

(i) f est continue sur I ;
(ii) $\Re e(f)$ et $\Im m(f)$ sont continues sur I ;
(iii) $\overline{f} : x \longmapsto \overline{f(x)}$ est continue sur I.

Preuve :

• Montrons $(i) \Longrightarrow (ii)$.
On suppose que f est continue sur I et on fixe $a \in I$. Alors f a une limite en a et d'après la proposition 6.2.2.11, $\Re e(f)$ et $\Im m(f)$ ont donc des limites en a, c'est-à-dire $\Re e(f)$ et $\Im m(f)$ sont continues en a. Ceci étant vrai pour tout $a \in I$, $\Re e(f)$ et $\Im m(f)$ sont continues sur I.

• Montrons $(ii) \Longrightarrow (iii)$.
On suppose que $\Re e(f)$ et $\Im m(f)$ sont continues sur I. Alors, $\mathcal{C}^0(I, \mathbb{C})$ étant un $\mathbb{C}$-espace vectoriel, $\Re e(f) - i\Im m(f)$ est continue sur I, c'est-à-dire $\overline{f}$ est continue sur I.

• Montrons enfin $(iii) \Longrightarrow (i)$.
On suppose que $\overline{f}$ est continue sur I et on fixe $a \in I$. On a alors pour tout $x \in I$:

$$|f(x) - f(a)| = |\overline{f(x) - f(a)}| = |\overline{f(x)} - \overline{f(a)}|$$

Or, $\lim\limits_{x \to a} \overline{f(x)} = \overline{f(a)}$ donc $\lim\limits_{x \to a} |\overline{f(x)} - \overline{f(a)}| = 0$, ce qui permet de conclure que $\lim\limits_{x \to a} |f(x) - f(a)| = 0$, c'est-à-dire $\lim\limits_{x \to a} f(x) = f(a)$.

⊠

Remarque : *on pouvait aussi remarquer que $(i) \iff (ii)$ toujours d'après la proposition 6.2.2.11 et ensuite conclure en remarquant que $\Im m(f)$ est continue si et seulement si $-\Im m(f)$ est continue.*

6.4.2 Composée de deux fonctions continues

Proposition 6.4.2.1 *Soient I et J deux intervalles de $\mathbb{R}$. Si $f : I \longrightarrow J$ et $g : J \longrightarrow \mathbb{K}$ sont deux fonctions continues sur I et J respectivement, alors $g \circ f$ est continue sur I.*

Preuve :

Soit $a \in I$. f est continue au point a donc f admet $f(a)$ pour limite en a. De plus, g est continue au point $f(a) \in J$, donc g admet $g(f(a))$ pour limite en $f(a)$. D'après la proposition 6.2.5.1 (composition de limites), $g \circ f$ admet $g(f(a))$ pour limite en a, c'est-à-dire $g \circ f$ est continue en a. Ceci étant vrai pour tout point $a \in I$, $g \circ f$ est continue sur I.

⊠

⚠ **Attention :** la proposition dit simplement que si l'on compose des applications continues, on obtient une application continue ! En revanche, on ne peut rien dire de

la composée d'une application continue et d'une application non continue, ou de deux applications non continues. Par exemple,

- $f : x \longmapsto \frac{1}{2+x^2}$ est continue sur $\mathbb{R}$, $g = E$ (partie entière) n'est pas continue sur $\mathbb{R}$ mais $g \circ f = 0$ est constante donc continue sur $\mathbb{R}$;
- $f = g = \chi_{[0,+\infty[}$, alors $g \circ f = 1$ est continue sur $\mathbb{R}$, alors que f (et donc g) ne sont pas continues en 0.

6.4.3 Restriction et caractère « local » de la continuité

Proposition 6.4.3.1 *Si f est continue sur I et $J \subset I$, alors $f_{|J}$ est continue sur J.*

Preuve :

Soit $a \in J$. Montrons que $f_{|J}$ est continue en a. Soit $(a_n)_{n\in\mathbb{N}} \in J^{\mathbb{N}}$ telle que $(a_n)_{n\in\mathbb{N}}$ converge vers a. Alors, la suite $(a_n)_{n\in\mathbb{N}}$ est aussi une suite d'éléments de I qui converge vers a et f est continue en a. D'après la caractérisation séquentielle de la continuité, $(f(a_n))_{n\in\mathbb{N}}$ converge vers $f(a)$. Or, pour tout entier $n \in \mathbb{N}$, $f(a_n) = f_{|J}(a_n)$ donc la suite $(f_{|J}(a_n))_{n\in\mathbb{N}}$ converge vers $f(a) = f_{|J}(a)$.
Ceci étant vrai pour toute suite $(a_n)_{n\in\mathbb{N}} \in J^{\mathbb{N}}$ de limite a, on en déduit que $f_{|J}$ est continue en a.
Et à nouveau, ceci étant vrai pour tout $a \in J$, $f_{|J}$ est continue sur J.

⊠

La proposition suivante ne sera pas réellement utile dans ce chapitre mais le sera dans le cours sur les séries de fonctions ou sur les intégrales à paramètre (voir cours de mathématiques spéciales 1, respectivement 2).

Proposition 6.4.3.2 *Si f est continue sur tout segment inclus dans I, alors f est continue sur I. On dit que la continuité est une propriété locale.*

Preuve :

C'est évident car si $a \in \overset{\circ}{I}$, il existe $r > 0$ tel que $[a-r, a+r] \subset I$ et la continuité sur $[a-r, a+r]$ implique la continuité de f en a. Si a est une borne (fermée) de I, on procède de même sur un intervalle $[a, a+r]$ si $a = \min I$ et $[a-r, a]$ si $a = \max I$.

⊠

6.4.4 Prolongement par continuité

Proposition 6.4.4.1 *Soient I un intervalle d'intérieur non vide, $f : I \longrightarrow \mathbb{K}$ et $a \in \overline{I} \setminus I$ et $a \in \mathbb{R}$ (c'est-à-dire a est une borne ouverte et finie de l'intervalle I). On suppose que $\lim\limits_{x \to a} f(x) = \ell$ avec $\ell \in \mathbb{K}$ (autrement dit, on suppose que f a une limite (finie) en a). Alors on peut prolonger f par continuité en a en posant :*

$$\begin{array}{rccl} \bar{f} : I \cup \{a\} & \longrightarrow & \mathbb{K} & \\ x & \longmapsto & \left\{ \begin{array}{ll} f(x) & si\ x \neq a \\ \ell & si\ x = a \end{array} \right. \end{array}$$

L'application $\bar{f}$ est l'unique prolongement de f qui est continu en a.

Preuve :

• Montrons pour commencer que $\bar{f}$ est continue en a.

Soit $\varepsilon > 0$. Par définition de la limite, il existe $\alpha > 0$ tel que :

$$\forall x \in I \cap [a - \alpha, a + \alpha] \ , \ |f(x) - \ell| \leqslant \varepsilon$$

Soit $x \in (I \cup \{a\}) \cap [a - \alpha, a + \alpha]$. On a alors deux cas :

- si $x = a$, alors $\bar{f}(x) = \ell$ donc $|\bar{f}(x) - \ell| \leqslant \varepsilon$;
- si $x \neq a$, alors $\bar{f}(x) = f(x)$ donc $|\bar{f}(x) - \ell| = |f(x) - \ell| \leqslant \varepsilon$.

Ce qui prouve que :

$$\forall \varepsilon > 0 \ , \ \exists \alpha > 0 \ , \ \forall x \in (I \cup \{a\}) \cap [a - \alpha, a + \alpha] \ , \ |\bar{f}(x) - \bar{f}(a)| \leqslant \varepsilon$$

c'est-à-dire que $\bar{f}$ est bien un prolongement de f qui est continu en a.

• Montrons à présent que c'est l'unique prolongement de f à $I \cup \{a\}$ qui est continu en a.
Soit g un prolongement de f à $I \cup \{a\}$ qui est continu en a. Par définition,

$$\forall x \in I \ , \ g(x) = f(x) = \bar{f}(x)$$

Par ailleurs, puisque g est continue en a, on a aussi :

$$g(a) = \lim_{\substack{x \to a \\ x \neq a}} g(x) = \lim_{\substack{x \to a \\ x \neq a}} f(x) = \ell = \bar{f}(a)$$

Par suite, $g = \bar{f}$.

⊠

Exemple 6.4.4.2 La fonction $f : \begin{array}{ccc}]0,+\infty[& \longrightarrow & \mathbb{R} \\ x & \longmapsto & x\sin\left(\frac{1}{x}\right) \end{array}$ se prolonge en une fonction continue sur $[0,+\infty[$ en posant $f(0) = 0$. En effet, $f(x) \underset{x\to 0^+}{=} O(x)$ donc d'après le théorème des gendarmes, $\lim\limits_{\substack{x\to 0 \\ x>0}} f(x) = 0$.
En revanche, cela n'a aucun sens de dire qu'on prolonge f par continuité en $+\infty$! Ici :

$$\sin\left(\frac{1}{x}\right) \underset{x\to+\infty}{\sim} \frac{1}{x} \quad \text{donc} \quad f(x) \underset{x\to+\infty}{\sim} 1$$

c'est-à-dire $\lim\limits_{x\to+\infty} f(x) = 1$, autrement dit f a bien une limite finie en $+\infty$ mais on ne peut pas prolonger par continuité en $+\infty$ car par définition, $\mathcal{D}_f \subset \mathbb{R}$.

Remarque : *attention, si f est définie sur $]a,b]$ avec $-\infty < a < b$, on peut toujours prolonger f à $[a,b]$ en posant $f(a) = 0$ (ou $f(a) = \pi$). Le théorème précédent parle uniquement de prolongement par continuité.*

Exercice 6.4.4.3 Soit $f :]a,b] \longrightarrow \mathbb{K}$, avec $(a,b) \in \mathbb{R}^2$ et $a < b$. Montrer que f a un prolongement continu en a si et seulement si f a une limite (finie si $\mathbb{K} = \mathbb{R}$) en a.

Corollaire 6.4.4.4 *Si $f \in \mathcal{C}^0(]a,b[,\mathbb{K})$ et si f admet des limites (finies) en a et en b, alors f admet un unique prolongement continu sur le segment $[a,b]$.*

Preuve :

C'est une conséquence directe de la proposition précédente.

⊠

⚠ **Attention :** le théorème ne s'applique pas tel quel en dehors d'une borne ouverte de l'intervalle. Autrement dit, si f est continue sur $\mathbb{R}^\star$ et f admet des limites finies à droite et à gauche en 0, on ne peut pas conclure qu'on peut prolonger f par continuité en 0 ! Il faut rajouter la condition « admet des limites finies à droite et à gauche en 0 qui sont égales ».

Par exemple, si $f : \begin{array}{ccc} \mathbb{R}^\star & \longrightarrow & \mathbb{R} \\ x & \longmapsto & \begin{cases} 1 & \text{si } x > 0 \\ -1 & \text{si } x < 0 \end{cases} \end{array}$, alors :

- $\lim\limits_{\substack{x\to 0 \\ x>0}} f(x) = 1$ donc on peut prolonger f par continuité sur $[0,+\infty[$;
- $\lim\limits_{\substack{x\to 0 \\ x<0}} f(x) = -1$ donc on peut prolonger f par continuité sur $]-\infty,0]$;
- en revanche, on ne peut pas prolonger f par continuité sur $\mathbb{R}$.

6.4.5 Théorème des valeurs intermédiaires

⚠ **Attention :** dans ce paragraphe, les fonctions considérées sont à valeurs réelles uniquement ! ! Le théorème des valeurs intermédiaires ne s'applique absolument pas aux fonctions à valeurs complexes !

Théorème 6.4.5.1 (Valeurs intermédiaires) *Soit I un intervalle d'intérieur non vide et soit $f : I \longrightarrow \mathbb{R}$ une fonction continue. Alors $f(I)$ est un intervalle.*
Autrement dit, si $a, b \in I$ et si $k \in \mathbb{R}$ est compris entre $f(a)$ et $f(b)$, alors l'équation $f(x) = k$ admet au moins une solution dans I.

Corollaire 6.4.5.2 *Soient f continue sur l'intervalle I, à valeurs réelles, et $a, b \in I$ tels que $f(a)f(b) \leqslant 0$. Alors f s'annule au moins une fois sur I.*

Corollaire 6.4.5.3 *Soit f continue sur l'intervalle I, à valeurs réelles, et ne s'annulant pas sur I. Alors f garde un signe constant strict sur l'intervalle I.*

Preuve du théorème des valeurs intermédiaires :

On veut montrer que, sous les hypothèses du théorème, $f(I)$ est un intervalle, c'est-à-dire qu'on veut montrer que :

$$\forall (\alpha, \beta) \in f(I)^2 \ , \ (\alpha < \beta \Longrightarrow [\alpha, \beta] \subset f(I))$$

Soient $\alpha, \beta \in f(I)$ tels que $\alpha < \beta$ et soit $\gamma \in [\alpha, \beta]$. Montrons que $\gamma \in f(I)$.
Tout d'abord, par définition de l'ensemble $f(I)$, il existe $a, b \in I$ tels que $f(a) = \alpha$ et $f(b) = \beta$. Quitte à remplacer f par $x \longmapsto f(-x)$, on peut toujours supposer que $a < b$.

• Si $\gamma = \alpha$ ou $\gamma = \beta$, alors $\gamma \in \{f(a)\} \cup \{f(b)\} \subset f(I)$ et le résultat est prouvé.
• On suppose à présent que $\alpha < \gamma < \beta$ et on considère l'ensemble :

$$E = \{x \in [a, b] \ , \ f(x) \leqslant \gamma\}$$

E est une partie non vide (elle contient a) et majorée (par b) de $\mathbb{R}$: elle admet donc une borne supérieure dans $\mathbb{R}$. Soit $c = \sup E$. Montrons que $f(c) = \gamma$.

* Tout d'abord, d'après la caractérisation de la borne supérieure dans $\mathbb{R}$, pour tout entier $n > 0$, il existe $x_n \in]c - \frac{1}{n}, c]$ tel que $x_n \in E$. Ceci définit une suite (x_n) d'éléments de $E \subset [a, b]$.
  D'après le théorème des gendarmes, (x_n) converge vers c et par définition de E :
  $$\forall n \in \mathbb{N}^\star \ , \ f(x_n) \leqslant \gamma$$
  Par continuité de f en c, on obtient, en passant à la limite :
  $$f(c) \leqslant \gamma$$

* Ensuite, d'après ce qui précède $c \in E$ et donc $c = \max E$. On en déduit donc que $c < b$ (puisque $b \notin E$). Pour tout entier $n \geqslant n_1$ (avec $n_1 = E(\frac{1}{b-c})+1$), $c+\frac{1}{n} \in [a, b]$ et est strictement plus grand que $\sup E$. Par suite, $c + \frac{1}{n} \notin E$, c'est-à-dire : $f(c + \frac{1}{n}) > \gamma$. En passant à la limite, on obtient (par continuité de f en c) :
  $$f(c) \geqslant \gamma$$

Par conséquent, $f(c) = \gamma$ avec $c \in [a, b] \subset I$.

⊠

Remarque : *on peut aussi utiliser l'algorithme de dichotomie pour déterminer une solution de $f(x) = k = \gamma$. Cet algorithme s'effectue de la façon suivante :*

- *on pose $a_0 = a$, $b_0 = b$, et $c_0 = \frac{a_0+b_0}{2}$;*
- *si $f(a_0) \leqslant \gamma \leqslant f(c_0)$, on pose $a_1 = a_0$, $b_1 = c_0$ et $c_1 = \frac{a_1+b_1}{2}$;*
- *sinon, on pose $a_1 = c_0$, $b_1 = b_0$ et $c_1 = \frac{a_1+b_1}{2}$;*
- *on recommence.*

On construit ainsi une suite de segments emboîtés $([a_n, b_n])$ dont le diamètre tend vers 0 et tels que :
$$\forall n \in \mathbb{N} \ , \ f(a_n) \leqslant \gamma \leqslant f(b_n)$$
D'après le théorème des segments emboîtés, $\bigcap_{n\in\mathbb{N}} [a_n, b_n] = \{\ell\}$ et on vérifie que $f(\ell) = \gamma$.
L'avantage de cette méthode est qu'elle permet dans la pratique de déterminer une valeur approchée d'une solution de l'équation $f(x) = \gamma$.

Exercice 6.4.5.4 Rédiger proprement la démonstration proposée en remarque.

Application : programmation de l'algorithme

Prenons par exemple le cas de la fonction f définie par $f(x) = x^3 + x - 1$ et $a = 0$ et $b = 1$. On peut alors saisir les instructions suivantes sous Scilab :

```
- -> function y = f(x) ;
y = x^3 + x - 1 ;
endfunction ;                                   (ceci permet de définir la fonction f)

function l=g(e)                                 (ici e désigne la précision)
a=0 ;b=1 ;                                      (affectation des variables a et b)
while (b-a>e)                                   (boucle « tant que »)
if f((a+b)/2)<0 then a=(a+b)/2 ;b=b ;           (boucle de test)
else a=a ;b=(a+b)/2 ;                           (suite de la boucle de test)
end ;                                           (fin de la boucle if)
end ;                                           (fin de la boucle while)
format(20) ;                                    (nombres de chiffres significatifs)
l=a                                             (le résultat que doit renvoyer le programme)
endfunction                                     (fin du programme)
```

⚠ **Attention :** le théorème des valeurs intermédiaires est faux pour une fonction à valeurs complexes ! Par exemple, si on considère la fonction f définie sur le segment $[0, \pi]$ par : $\forall x \in [0, \pi]$, $f(x) = e^{ix}$, alors f est clairement continue sur $[0, \pi]$ puisque cos et sin le sont. De plus, $f(0) = 1$ et $f(\pi) = -1$. On a bien $0 \in [-1, 1]$ et pourtant, l'équation $f(x) = 0$ n'a pas de solution !

Remarque : *la continuité est une condition suffisante, mais pas nécessaire, pour qu'une fonction vérifie la propriété des valeurs intermédiaires ! On verra en exercice que toute fonction dérivée vérifie la propriété des valeurs intermédiaires (théorème de Darboux, voir le chapitre de dérivation du cours de mathématiques supérieures 2).*

Preuve du premier corollaire (corollaire 6.4.5.2) :

Avec les hypothèses du corollaire, $0 \in [f(a), f(b)] \cup [f(b), f(a)]$. Or, d'après le théorème des valeurs intermédiaires, $f([a, b])$ est un intervalle et $(f(a), f(b)) \in f([a, b])^2$ donc $0 \in f([a, b])$, c'est-à-dire qu'il existe $c \in [a, b]$ tel que $0 = f(c)$.

⊠

Preuve du second corollaire (corollaire 6.4.5.3) :

Si f ne garde pas un signe constant strict, alors il existe $(a, b) \in I^2$ tel que $f(a)f(b) \leqslant 0$. D'après le premier corollaire, il existe $c \in I$ tel que $f(x) = 0$, ce qui est absurde.

⊠

6.4.6 Image d'un segment par une fonction continue

Théorème 6.4.6.1 *Soient a, b deux réels tels que $a \leqslant b$ et soit $f : [a,b] \longrightarrow \mathbb{R}$ une fonction continue et à valeurs réelles. Alors $f([a,b])$ est un segment. Autrement dit, il existe deux réels m et M tels que $m \leqslant M$ et $f([a,b]) = [m,M]$.*
En particulier, f est bornée sur $[a,b]$ et atteint ses bornes sur $[a,b]$, c'est-à-dire :

$$\sup_{x\in[a,b]} f(x) = \max_{x\in[a,b]} f(x) \quad \text{et} \quad \inf_{x\in[a,b]} f(x) = \min_{x\in[a,b]} f(x)$$

Preuve :

D'après le théorème des valeurs intermédiaires (qui s'applique puisque f est continue sur $I = [a,b]$ et est à valeurs réelles), $f([a,b])$ est un intervalle.

• Montrons que $f([a,b])$ est majoré et que $\sup_{x\in[a,b]} f(x) = \max_{x\in[a,b]} f(x)$.

∗ Si f n'est pas majorée sur $[a,b]$, alors :

$$\forall n \in \mathbb{N}\ ,\ \exists x_n \in [a,b]\ ,\ f(x_n) \geqslant n$$

Pour chaque entier n, on fixe un tel x_n, ce qui définit une suite $(x_n)_{n\in\mathbb{N}}$ d'éléments de $[a,b]$. La relation précédente montre directement que $\lim_{n\to+\infty} f(x_n) = +\infty$.
Par ailleurs, puisque pour tout entier n, $x_n \in [a,b]$, la suite $(x_n)_{n\in\mathbb{N}}$ est une suite réelle bornée. D'après le théorème de Bolzano-Weierstrass, il existe une suite extraite $(x_{\varphi(n)})_{n\in\mathbb{N}}$ qui converge. Notons ℓ la limite de $(x_{\varphi(n)})$. On a alors :

▷ d'une part : $\forall n \in \mathbb{N}\ ,\ x_{\varphi(n)} \in [a,b]$. En passant à la limite, $\ell \in [a,b]$. De plus, par continuité de f en ℓ :

$$\lim_{n\to+\infty} f(x_{\varphi(n)}) = f(\ell)$$

▷ d'autre part, $\forall n \in \mathbb{N}\ ,\ f(x_{\varphi(n)}) \geqslant \varphi(n) \geqslant n$. Par suite,

$$\lim_{n\to+\infty} f(x_{\varphi(n)}) = +\infty$$

Ainsi, $(f(x_{\varphi(n)}))_{n\in\mathbb{N}}$ converge vers $f(\ell)$ et diverge vers $+\infty$, ce qui est absurde. Par conséquent, f est majorée sur $[a,b]$.

∗ Ainsi, $\{f(x)\ ,\ x \in [a,b]\}$ est un intervalle non vide et majoré de $\mathbb{R}$, il admet donc une borne supérieure dans $\mathbb{R}$.

Posons $M = \sup\{f(x)\ ,\ x \in [a,b]\}$ et montrons que M est en fait un maximum.
D'après la caractérisation de la borne supérieure dans $\mathbb{R}$:

$$\forall n \in \mathbb{N}\ ,\ \exists t_n \in [a,b]\ ,\ M - \frac{1}{n+1} < f(t_n) \leqslant M$$

Pour chaque entier n, on fixe un tel réel t_n, ce qui définit à nouveau une suite réelle bornée (t_n). Toujours d'après le théorème de Bolzano-Weierstrass, il existe une suite extraite $(t_{\psi(n)})_{n\in\mathbb{N}}$ qui converge. Sa limite c appartient à $[a,b]$ et on a :

$$\forall n \in \mathbb{N}\ ,\ M - \frac{1}{\psi(n)+1} < f(t_{\psi(n)}) \leqslant M$$

Or, f est continue en c et $\lim\limits_{n\to+\infty} \psi(n) = +\infty$: d'après le théorème des gendarmes, $f(c) = \lim\limits_{n\to+\infty} f(t_{\psi(n)}) = M$.
Par suite, $M \in \{f(x)\ ,\ x \in [a,b]\}$, c'est-à-dire $M = \max\limits_{x\in[a,b]} f(x)$.

• En appliquant ce qui précède à $-f$ (qui vérifie bien les mêmes hypothèses que f), on en déduit que f est également minorée sur $[a,b]$ et que $\inf\{f(x)\ ,\ x \in [a,b]\} = \min\{f(x)\ ,\ x \in [a,b]\}$.

⊠

Remarques :

- *pour raccourcir la démonstration, on aurait pu définir $M = \sup_{[a,b]} f$ dans $\overline{\mathbb{R}}$ et introduire directement une suite (x_n) d'éléments de $[a,b]$ avec $\lim\limits_{n\to+\infty} f(x_n) = M$ (toujours dans $\overline{\mathbb{R}}$). La même méthode montre alors que $M = f(c)$: donc M est fini et $M \in f([a,b])$.*
- *souvent, on énonce ce théorème sous l'une des deux formes suivantes :*
  (i) l'image d'un segment par une fonction continue est un segment ;
  (ii) toute fonction continue sur un segment est bornée et atteint ses bornes.
  Attention, dans cette formulation, on n'a jamais précisé que f est à valeurs réelles !

Exemple 6.4.6.2 Soit $T > 0$ et soit f une fonction continue sur $\mathbb{R}$, T-périodique, à valeurs réelles. Montrons que f est bornée sur $\mathbb{R}$ et qu'elle atteint ses bornes.

• Puisque f est continue sur $\mathbb{R}$, elle l'est aussi sur le segment $[0,T]$. Par conséquent, f est bornée et atteint ses bornes sur le segment $[0,T]$. Autrement dit, il existe $a \in [0,T]$ et $b \in [0,T]$ tels que :

$$f(a) = \min_{x\in[0,T]} f(x) \quad \text{et} \quad f(b) = \max_{x\in[0,T]} f(x)$$

• Montrons alors que : $\forall x \in \mathbb{R}$, $f(a) \leqslant f(x) \leqslant f(b)$.

Soit $x \in \mathbb{R}$. Posons $n = E\left(\frac{x}{T}\right)$. Alors par définition, $n \leqslant \frac{x}{T} < n+1$ et donc :

$$(x - nT) \in [0, T[\subset [0, T]$$

Il s'ensuit que :

$$f(a) \leqslant f(x - nT) \leqslant f(b)$$

Or, f est T-périodique donc $f(x - nT) = f(x)$ et finalement, $f(a) \leqslant f(x) \leqslant f(b)$.

Exercice 6.4.6.3 Soit $f : [0,1] \longrightarrow \mathbb{R}$ continue telle que : $\forall x \in [0,1]$, $f(x) > 0$. Montrer que :

$$\exists \varepsilon > 0 \ , \forall x \in [0,1] \ , \ f(x) \geqslant \varepsilon$$

Théorème 6.4.6.4 *Soient $a \leqslant b$ deux réels et $f : [a,b] \longrightarrow \mathbb{C}$ une fonction continue. Alors f est bornée sur $[a,b]$ et de plus, $|f|$ atteint ses bornes sur $[a,b]$:*

$$\sup_{x\in[a,b]} |f(x)| = \max_{x\in[a,b]} |f(x)| \quad \text{et} \quad \inf_{x\in[a,b]} |f(x)| = \min_{x\in[a,b]} |f(x)|$$

Preuve :

Il suffit d'appliquer le théorème précédent à la fonction $|f|$ qui est continue sur le segment $[a,b]$ (car f l'est) et à valeurs réelles.

⊠

Remarque : *ce résultat sera généralisé dans le cours de mathématiques spéciales 1 : « l'image d'un compact par une application continue est un compact ».*

6.4.7 Continuité de la bijection réciproque

Théorème 6.4.7.1 *Soit f une application strictement monotone et continue sur I. Alors f réalise une bijection de I sur l'intervalle $J = f(I)$ et sa bijection réciproque $f^{-1} : J \longrightarrow I$ est continue sur J.*

La preuve de la continuité de f^{-1} est admise, la voici pour ceux qui sont intéressés.

Preuve :

Il reste seulement à prouver la continuité de f^{-1}. Quitte à travailler avec $-f$, on peut toujours supposer que f est strictement croissante.
Soit $b \in J$ et $a \in I$ tel que $b = f(a)$. Montrons que f^{-1} est continue en b. On suppose que b n'est pas une borne de l'intervalle J. On fixe $\varepsilon > 0$ que l'on choisit tel que $[a-\varepsilon, a+\varepsilon] \subset I$. On a alors pour tout $y \in J$:

$$\begin{aligned} |f^{-1}(y) - f^{-1}(b)| \leqslant \varepsilon &\iff a - \varepsilon \leqslant f^{-1}(y) \leqslant a + \varepsilon \\ &\iff f(a-\varepsilon) \leqslant y \leqslant f(a+\varepsilon) \end{aligned}$$

La fonction f étant strictement croissante, on a

$$f(a-\varepsilon) < f(a) < f(a+\varepsilon)$$

Il existe alors un réel $\alpha > 0$ tel que $[f(a)-\alpha, f(a)+\alpha] \subset [f(a-\varepsilon), f(a+\varepsilon)]$, c'est-à-dire $[b-\alpha, b+\alpha] \subset [f(a-\varepsilon), f(a+\varepsilon)]$.
On a pour un tel α :

$$\forall y \in J \ , \ |y-b| \leqslant \alpha \Longrightarrow |f^{-1}(y) - f^{-1}(b)| \leqslant \varepsilon$$

⊠

Corollaire 6.4.7.2 *Si $f : I \longrightarrow J$ (avec I, J deux intervalles) est continue et bijective, alors f^{-1} est continue.*

Preuve :

On verra en exercice que si f est continue, alors f est injective si et seulement si f est strictement monotone. On peut donc appliquer le théorème précédent.

⊠

6.4.8 Continuité uniforme et théorème de Heine

La notion de continuité uniforme n'est pas un objectif principal de ce chapitre. Essentiellement, cette notion est importante pour démontrer les théorèmes d'approximations comme le théorème de Weierstrass (voir cours sur les suites et séries de fonctions (mathématiques spéciales 1)) ou l'approximation des fonctions continues par morceaux sur un segment par des fonctions en escalier (voir cours d'intégration (cours de mathématiques supérieures 2)). Elle est aussi importante dans d'autres domaines par application du théorème de prolongement des applications uniformément continues. En ce qui nous concerne, ce paragraphe peut être omis en première lecture.

Définition 6.4.8.1 Soit I un intervalle et soit $f : I \longrightarrow \mathbb{K}$. On dit que f est uniformément continue sur I si :

$$\forall \varepsilon > 0 \ , \ \exists \alpha > 0 \ , \ \forall (x,y) \in I^2 \ , \ |x-y| \leqslant \alpha \Longrightarrow |f(x) - f(y)| \leqslant \varepsilon$$

Exercice 6.4.8.2 Quelle est la différence avec la définition de f continue sur I ? Du coup, justifiez le choix du mot « uniformément ».

Exemple 6.4.8.3 Les fonctions affines sont uniformément continues sur $\mathbb{R}$. En effet, si $(a,b) \in \mathbb{R}^2$, alors pour tout $\varepsilon > 0$, en posant $\alpha = \frac{\varepsilon}{|a|+1}$, on a pour tout $(x,y) \in \mathbb{R}^2$:

$$\begin{array}{rcl} |x-y| \leqslant \alpha & \Longrightarrow & |(ax+b) - (ay+b)| \leqslant |a| \times \alpha \\ & \Longrightarrow & |(ax+b) - (ay+b)| \leqslant \varepsilon \end{array}$$

Exercice 6.4.8.4 Montrer que sin est uniformément continue sur $\mathbb{R}$.

Proposition 6.4.8.5 *Soit $f : I \longrightarrow \mathbb{K}$. Alors les énoncés suivants sont équivalents :*

(i) f est uniformément continue sur l'intervalle I ;

(ii) pour toutes suites $(x_n)_{n\in\mathbb{N}}, (y_n)_{n\in\mathbb{N}} \in I^{\mathbb{N}}$ telles que $(y_n - x_n)$ converge vers 0, la suite $(f(y_n) - f(x_n))_{n\in\mathbb{N}}$ converge vers 0.

Preuve :

• Montrons $(i) \Longrightarrow (ii)$

On suppose que f est uniformément continue sur I. Montrons (ii).
Soient $(x_n)_{n\in\mathbb{N}}$ et $(y_n)_{n\in\mathbb{N}}$ deux suites d'éléments de I telles que $\lim\limits_{n\to+\infty} (y_n - x_n) = 0$. Montrons que $(f(y_n) - f(x_n))_{n\in\mathbb{N}}$ converge vers 0.

Soit $\varepsilon > 0$. Par hypothèse, f est uniformément continue sur I donc :

$$\exists \alpha > 0 \ , \ \forall (x,y) \in I^2 \ , \ |x-y| \leqslant \alpha \Longrightarrow |f(x) - f(y)| \leqslant \varepsilon$$

Soit un tel réel $\alpha > 0$. Toujours par hypothèse, $\lim\limits_{n\to+\infty} (x_n - y_n) = 0$. Il existe donc un entier n_0 tel que :

$$\forall n \geqslant n_0 \ , \ |x_n - y_n| \leqslant \alpha$$

Mais alors, puisque $(x_n)_{n\in\mathbb{N}}$ et $(y_n)_{n\in\mathbb{N}}$ sont des suites à valeurs dans I, on a :

$$\forall n \geqslant n_0 \ , \ |f(x_n) - f(y_n)| \leqslant \varepsilon$$

Ce qui prouve que $(f(x_n) - f(y_n))_{n\in\mathbb{N}}$ converge vers 0.

• Montrons $(ii) \Longrightarrow (i)$ par contraposée.

On suppose que f n'est pas uniformément continue sur I, c'est-à-dire :

$$\exists \varepsilon > 0 \ , \ \forall \alpha > 0 \ , \ \exists (x,y) \in I^2 \ , \ |x-y| \leqslant \alpha \ \text{ et } \ |f(x) - f(y)| > \varepsilon$$

On fixe un réel $\varepsilon > 0$ vérifiant la propriété ci-dessus. Pour tout entier $n \in \mathbb{N}^\star$, on choisit $\alpha = \frac{1}{n}$: il existe $x_n, y_n \in I$ tels que : $|x_n - y_n| \leqslant \frac{1}{n}$ et $|f(x_n) - f(y_n)| > \varepsilon$.

Ceci définit deux suites (x_n) et (y_n), d'éléments de I, qui vérifient :

- $\forall n \in \mathbb{N}^\star \ , \ |x_n - y_n| \leqslant \frac{1}{n}$ donc $\lim\limits_{n\to+\infty} (x_n - y_n) = 0$;
- $\forall n \in \mathbb{N}^\star \ , \ |f(x_n) - f(y_n)| > \varepsilon$. Par conséquent, $(f(x_n) - f(y_n))$ ne peut pas converger vers 0.

Ce qui prouve la propriété non (ii).

⊠

Proposition 6.4.8.6 *Soit $f : I \longrightarrow \mathbb{K}$ une fonction définie sur l'intervalle I. Alors :*

$$f \text{ lipschitzienne} \Longrightarrow f \text{ uniformément continue} \Longrightarrow f \text{ continue}$$

De plus, chacune des réciproques est fausse.

Preuve :

• Montrons f lipschitzienne $\Longrightarrow f$ uniformément continue .
On suppose que f est k-lipschitzienne sur I avec $k \geqslant 0$.
Soient $\varepsilon > 0$ et $\alpha = \frac{\varepsilon}{k+1} > 0$. Pour tout $(x,y) \in I^2$ tel que $|x-y| \leqslant \alpha$,

$$|f(x) - f(y)| \leqslant k|x-y| \leqslant k\alpha \leqslant \varepsilon$$

Ce qui prouve que f est uniformément continue sur I.

• L'implication f uniformément continue $\Longrightarrow f$ continue est évidente. En effet, supposons que f soit uniformément continue sur I et fixons $a \in I$. Soit $\varepsilon > 0$. Il existe $\alpha > 0$ tel que :

$$\forall (x,y) \in I^2 \ , \ |x-y| \leqslant \alpha \Longrightarrow |f(x) - f(y)| \leqslant \varepsilon$$

En particulier,

$$\forall x \in I \ , \ |x-a| \leqslant \alpha \Longrightarrow |f(x)-f(a)| \leqslant \varepsilon$$

Ce qui prouve que f est continue au point a.

• Montrons que les réciproques sont fausses.

∗ Montrons que $x \longmapsto \sqrt{x}$ est uniformément continue sur $[0,1]$ mais pas lipschitzienne.

▷ Soit $\varepsilon > 0$. Posons $\alpha = \varepsilon^2 > 0$. Alors, pour tout $(x,y) \in [0,1]^2$ tel que $|x-y| \leqslant \alpha$,

– si $\sqrt{x}+\sqrt{y} \leqslant \varepsilon$, alors $|\sqrt{x}-\sqrt{y}| \leqslant \sqrt{x}+\sqrt{y} \leqslant \varepsilon$;

– si $\sqrt{x}+\sqrt{y} > \varepsilon$, alors :

$$|\sqrt{x}-\sqrt{y}| = \frac{|x-y|}{\sqrt{x}+\sqrt{y}} < \frac{|x-y|}{\varepsilon} \leqslant \varepsilon$$

Ce qui prouve que $x \longmapsto \sqrt{x}$ est uniformément continue sur $[0,1]$.

▷ Pour tout $x \in]0,1]$, $\dfrac{|\sqrt{x}-\sqrt{0}|}{|x-0|} = \dfrac{1}{\sqrt{x}}$. Or, $\lim\limits_{\substack{x\to 0\\ x>0}} \dfrac{1}{\sqrt{x}} = +\infty$ donc $x \longmapsto \dfrac{|\sqrt{x}-\sqrt{0}|}{|x-0|}$ n'est pas majorée sur $]0,1]$.

Ce qui prouve que $x \longmapsto \sqrt{x}$ n'est pas lipschitzienne sur $[0,1]$.

∗ Montrons que $x \longmapsto x^2$ est continue sur $\mathbb{R}$ mais pas uniformément continue sur $\mathbb{R}$.

La continuité est évidente. Pour montrer qu'elle n'est pas uniformément continue, on utilise la caractérisation séquentielle. Soit $(x_n)_{n\in\mathbb{N}}$ et $(y_n)_{n\in\mathbb{N}}$ définies par :

$$\forall n \in \mathbb{N} \ , \ x_n = n+1 \ \text{ et } \ y_n = x_n + \frac{1}{n+1}$$

Alors :

▷ $\lim\limits_{n\to+\infty} (x_n - y_n) = 0$;

▷ pour tout $n \in \mathbb{N}$, $y_n^2 - x_n^2 = 2 + \frac{1}{(n+1)^2}$ donc la suite $(y_n^2 - x_n^2)$ ne converge pas vers 0.

Ainsi, $x \longmapsto x^2$ n'est pas uniformément continue sur $\mathbb{R}$. ⊠

Exercice 6.4.8.7 Proposer une autre preuve de la seconde implication, à l'aide de suites.

Théorème 6.4.8.8 (Heine) *Toute fonction continue sur un segment, à valeurs réelles ou complexes, est uniformément continue sur ce segment.*

Preuve :

Soient $a < b$ deux réels et $f : [a,b] \longrightarrow \mathbb{K}$ une fonction continue sur $[a,b]$. Montrons que f est uniformément continue sur $[a,b]$ en raisonnant par l'absurde.
Supposons que f ne soit pas uniformément continue sur $[a,b]$. Alors :

$$\exists \varepsilon > 0 \ , \ \forall \alpha > 0 \ , \ \exists (x,y) \in [a,b]^2 \ , \ |x-y| \leqslant \alpha \text{ et } |f(x)-f(y)| > \varepsilon$$

On fixe un tel $\varepsilon > 0$ et, comme dans la preuve de la proposition précédente, on choisit pour $n \in \mathbb{N}$, x_n, y_n deux éléments de $[a,b]$ tels que :

$$|x_n - y_n| \leqslant \frac{1}{n+1} \quad \text{et} \quad |f(x_n) - f(y_n)| > \varepsilon$$

La suite $(x_n)_{n\in\mathbb{N}}$ est bornée (et réelle) : d'après le théorème de Bolzano-Weierstrass, il existe une suite extraite $(x_{\varphi_1(n)})$ de (x_n) qui converge vers ℓ et $\ell \in [a,b]$.
Ensuite, on considère la suite $(y_{\varphi_1(n)})$: cette suite est également réelle et bornée donc il existe une suite extraite $(y_{(\varphi_1\circ\varphi_2)(n)})$ de $(y_{\varphi_1(n)})$ qui converge vers ℓ' avec $\ell' \in [a,b]$.
On pose $\varphi = \varphi_1 \circ \varphi_2$ (qui est bien une extraction, c'est-à-dire une application strictement croissante de $\mathbb{N}$ dans $\mathbb{N}$) : par construction $(y_{\varphi(n)})$ converge vers ℓ' et $(x_{\varphi(n)})$ converge vers ℓ (car c'est une suite extraite de la suite convergente $(x_{\varphi_1(n)})$).
Or, $\forall n \in \mathbb{N}$, $|x_{\varphi(n)} - y_{\varphi(n)}| \leqslant \frac{1}{\varphi(n)+1} \leqslant \frac{1}{n+1}$ avec $\lim\limits_{n\to+\infty} \dfrac{1}{n+1} = 0$ donc $\ell = \ell'$.
Ainsi, $(x_{\varphi(n)})$ et $(y_{\varphi(n)})$ convergent vers la même limite $\ell \in [a,b]$. Or, f est continue en ℓ donc d'après la caractérisation séquentielle de la limite, $(f(x_{\varphi(n)}))$ et $(f(y_{\varphi(n)}))$ convergent toutes les deux vers $f(\ell)$, et par conséquent, la suite $(f(x_{\varphi(n)}) - f(y_{\varphi(n)}))$ converge vers 0. Ceci contredit le fait que :

$$\forall n \in \mathbb{N} \ , \ |f(x_{\varphi(n)}) - f(y_{\varphi(n)})| > \varepsilon$$

⊠

Remarque : *notez bien au passage que dans la preuve, on a démontré que si $(x_n)_{n\in\mathbb{N}}$ et $(y_n)_{n\in\mathbb{N}}$ sont deux suites réelles bornées, alors il existe une extraction φ telle que $(x_{\varphi(n)})$ et*

$(y_{\varphi(n)})$ convergent. Ceci fournit une preuve du théorème de Bolzano-Weierstrass pour une suite complexe. En effet, si $(z_n)_{n\in\mathbb{N}} \in \mathbb{C}^{\mathbb{N}}$ est bornée, alors les suites $(x_n) = (\Re e(z_n))$ et $(y_n) = (\Im m(z_n))$ sont bornées et donc on peut extraite simultanément $(x_{\varphi(n)})$ et $(y_{\varphi(n)})$ qui convergent. Alors $(z_{\varphi(n)})$ converge car ses parties réelle et imaginaire sont convergentes.

Remarque : *on retrouve donc aussi de façon immédiate que $x \longmapsto \sqrt{x}$ est uniformément continue sur $[0,1]$ car c'est une fonction continue sur un segment.*

6.5 Bilan sur les différences entre fonctions à valeurs réelles ou complexes

Dans les parties précédentes, on a déjà traité les fonctions à valeurs complexes. Attention, ce sont encore des fonctions d'une variable réelle ! La seule différence est que les valeurs prises par ces fonctions sont des nombres complexes. On résume ici les définitions et propriétés qui restent valables pour les fonctions à valeurs complexes et celles qui ne le sont plus (c'est-à-dire qui sont spécifiques aux fonctions à valeurs réelles).

Essentiellement, c'est facile à retenir : les propriétés ou définitions faisant intervenir la relation d'ordre dans $\mathbb{R}$ sont fausses sur $\mathbb{C}$.

1. Pour une fonction $f : I \longrightarrow \mathbb{C}$, on définit les fonctions réelles :
   (a) la fonction partie réelle de f : $\begin{array}{rcl} \Re e(f) : I & \longrightarrow & \mathbb{R} \\ x & \longmapsto & \Re e(f(x)) \end{array}$
   (b) la fonction partie imaginaire de f : $\begin{array}{rcl} \Im m(f) : I & \longrightarrow & \mathbb{R} \\ x & \longmapsto & \Im m(f(x)) \end{array}$
   (c) la fonction module de f : $\begin{array}{rcl} |f| : I & \longrightarrow & \mathbb{R}^+ \\ x & \longmapsto & |f(x)| \end{array}$
   (d) on peut aussi définir la fonction conjuguée de f qui est à valeurs complexes :
   $$\begin{array}{rcl} \overline{f} : I & \longrightarrow & \mathbb{C} \\ x & \longmapsto & \overline{f(x)} \end{array}$$
2. Soit $f : I \longrightarrow \mathbb{C}$. On dit que f est bornée si :
   $$\exists M \geqslant 0 \ , \ \forall x \in I \ , \ |f(x)| \leqslant M$$
3. Soient $f : I \longrightarrow \mathbb{C}$, $a \in \overline{I}$ et $\ell \in \mathbb{C}$. On dit que f admet ℓ pour limite en a si :
   $$\forall \varepsilon > 0 \ , \ \exists V \in \mathcal{V}_f(a) \ , \ \forall x \in I \cap V \ , \ |f(x) - \ell| \leqslant \varepsilon$$

4. Si f admet une limite en a, alors cette limite est unique.
5. Soient $f : I \longrightarrow \mathbb{C}$ et $a \in \overline{I}$. Alors :

   f admet une limite en $a \iff \Re e(f)$ et $\Im m(f)$ admettent des limites finies en a

   Dans ce cas, $\lim\limits_{x\to a} f(x) = \lim\limits_{x\to a} (\Re e(f)(x)) + i \times \lim\limits_{x\to a} (\Im m(f)(x))$.
6. Si f admet une limite en a, alors f est bornée au voisinage de a.
7. L'arithmétique des limites reste valable pour les fonctions à valeurs complexes.
8. On dit que f est continue en $a \in I$ si f admet une limite en a. Dans ce cas, cette limite est nécessairement $f(a)$.
9. La caractérisation séquentielle (par les suites) de la limite (ou de la continuité) est encore valable.
10. Théorème de comparaison : si pour tout x proche de a, $|f(x)| \leqslant g(x)$, avec g une fonction à valeurs réelles et positives, et si $\lim\limits_{x\to a} g(x) = 0$, alors $\lim\limits_{x\to a} f(x) = 0$.
11. La définition d'une fonction lipschitzienne reste valable.
12. Si $f : [a, b] \longrightarrow \mathbb{C}$ est continue, alors $|f|$ est bornée et atteint ses bornes sur $[a, b]$.
13. La définition de l'uniforme continuité reste valable.
14. Le théorème de Heine reste valable.
15. Les définitions et propriétés avec les o, O et $\sim$ restent valables (sauf les propriétés de signe).

⚠ **Attention :** en revanche, tous les théorèmes ou définitions faisant intervenir la relation d'ordre dans $\mathbb{R}$ sont faux. Par exemple,

1. La notion de fonction complexe monotone n'a aucun sens !
2. La notion de fonction complexe majorée (ou minorée) n'a aucun sens !
3. Le théorème de la limite monotone n'est plus valable !
4. Le théorème des valeurs intermédiaires ne s'applique pas !
5. L'image d'un segment par une fonction continue à valeurs complexes n'est plus un segment !

6.6 Exercices

Exercice 6.6.1 En revenant à la définition formelle, montrer que $\lim_{x\to 1} \dfrac{x}{\sqrt{x^2+3}} = \dfrac{1}{2}$.

Exercice 6.6.2 Démontrer que toute fonction définie sur $\mathbb{R}$, périodique et admettant une limite en $+\infty$ est constante.

Exercice 6.6.3 Soit I un intervalle d'intérieur non vide.

1. On suppose que I est borné. Montrer que si f est une fonction lipschitzienne sur I, alors f est bornée.
2. En déduire que si I est borné, alors le produit de deux fonctions lipschitziennes sur I est encore une fonction lipschitzienne.
3. Montrer que le résultat de la question 2 n'est pas toujours vrai si I n'est pas borné.

Exercice 6.6.4 Étudier la continuité de f définie sur $\mathbb{R}$ par : $f(x) = \begin{cases} x & \text{si } x \in \mathbb{Q} \\ 1-x & \text{sinon} \end{cases}$.
La fonction f est-elle bijective ?

Exercice 6.6.5 Étudier les limites aux bornes et la continuité des applications suivantes :

$$f(x) = E(x) \ ; \ g(x) = E\left(\frac{1}{x}\right) \ ; \ h(x) = (-1)^{E(x)}(x - E(x)) \ ; \ l(x) = E(x) + \sqrt{x - E(x)}$$

Exercice 6.6.6 Déterminer les fonctions continues en 0, à valeurs dans $\mathbb{R}$, vérifiant : $\forall x, y \in \mathbb{R}$, $f(x+y) = f(x)f(y)$.

Exercice 6.6.7 Déterminer les applications de $\mathbb{R}$ dans $\mathbb{R}$, continues en 0, et vérifiant la relation : $\forall x \in \mathbb{R}$, $f(2x) = f(x)$.

Exercice 6.6.8

1. Donner un exemple d'application $f : \mathbb{R} \longrightarrow \mathbb{R}$ non constante vérifiant la relation : $\forall x \in \mathbb{R}$, $f(x^2) = f(x)$.
2. Soit $f : \mathbb{R} \longrightarrow \mathbb{R}$ une application. On suppose que f est continue en 0 et en 1 et qu'elle vérifie la relation : $\forall x \in \mathbb{R}$, $f(x^2) = f(x)$. Montrer que f est constante.

Exercice 6.6.9 Déterminer toutes les applications f, continues de $\mathbb{R}$ dans $\mathbb{R}$, et vérifiant :

$$\forall (x,y) \in \mathbb{R}^2 \ , \ f(x+y) + f(x-y) = 2(f(x) + f(y))$$

Exercice 6.6.10 Trouver un équivalent simple en 0 des fonctions suivantes :

$$f(x) = \cos(\sin x) \ ; \ g(x) = \ln(\cos x) \ ; \ h(x) = \ln(\sin x) \ ; \ i(x) = \cos(ax) - \cos(bx)$$
$$j(x) = a^x - b^x \ ; \ k(x) = \arctan(\operatorname{sh} x) \ ; \ l(x) = \sqrt[4]{1+x^2} - \sqrt[4]{1-x^2}$$

Exercice 6.6.11 Déterminer un équivalent simple de chacune des fonctions en $+\infty$:

$$f(x) = \sin(e^{-x}) \ ; \ g(x) = \ln\cos\left(\frac{1}{x^2}\right) \ ; \ h(x) = \sqrt{x^2+x+1} - \sqrt{x^2-x+1}$$

Exercice 6.6.12 Calculer les limites suivantes en utilisant les équivalents :

$$\lim_{x\to 0} \ln(x)\tan(2x) \quad ; \quad \lim_{x\to 0} \frac{\ln(\cos(ax))}{\ln(\cos(bx))} \quad ; \quad \lim_{x\to 0} \frac{\ln(1+\tan x)}{1-\cos(2x)}$$

Exercice 6.6.13 Déterminer les limites suivantes :

$$\lim_{x\to \frac{1}{2}} (2x^2 - 3x + 1)\tan(\pi x) \quad ; \quad \lim_{x\to 0} \ln x \times \ln\Big(1 + \ln(1+x)\Big) \quad ; \quad \lim_{x\to 0} (1+\tan x)^{\frac{1}{\sin x}}$$

Exercice 6.6.14 Déterminer, si elles existent, les limites suivantes :

$$\lim_{\substack{x\to \frac{\pi}{2} \\ x<\frac{\pi}{2}}} \ln\left(\frac{2x}{\pi}\right)\exp\left(\frac{1}{\cos x}\right) \quad ; \quad \lim_{x\to 0} \operatorname{cotan}(x)\ln(1+\sin x) \quad ; \quad \lim_{x\to 0} \frac{\sin x \ln(1+x^2)}{x\tan x}$$

$$\lim_{x\to 0} \left(\frac{1}{x(x+1)e^x} - \frac{1}{x\cos x}\right) \quad ; \quad \lim_{\substack{x\to 0 \\ x>0}} (\cos x)^{\ln x} \quad ; \quad \lim_{x\to+\infty} \Big(\ln(1+e^{-x})\Big)^{\frac{1}{x}}$$

Exercice 6.6.15

1. Soient u et v deux fonctions équivalentes en a. Montrer que :
$$e^{u(x)} \underset{x\to a}{\sim} e^{v(x)} \iff u(x) - v(x) \underset{x\to a}{=} o(1)$$
2. On note $E(x)$ la partie entière d'un nombre réel x.
   (a) Soit $\alpha \in]0,1[$. Montrer que : $e^{E(x)^\alpha} \underset{x\to+\infty}{\sim} e^{x^\alpha}$. *On pourra utiliser la question 1.*
   (b) Montrer que si $\beta \geqslant 1$, alors $e^{E(x)^\beta}$ et e^{x^β} ne sont pas équivalents en $+\infty$.
   Indication : *on pourra introduire la suite* $(x_n) = (n + \frac{1}{2})$.

Exercice 6.6.16 Soit $f :]0, +\infty[\longrightarrow \mathbb{R}$ telle que f est croissante et $x \longmapsto \dfrac{f(x)}{x}$ est décroissante. Montrer que f est continue.

Exercice 6.6.17 Soit f une application de I dans $\mathbb{R}$. On suppose que f est monotone et que $f(I)$ est un intervalle. Montrer que f est continue.

Exercice 6.6.18 Soit $f : [0, 1] \longrightarrow [0, 1]$ continue. Montrer que f admet un point fixe.

Exercice 6.6.19 Soit f une fonction continue sur $[0, 1]$, à valeurs réelles, et telle que $f(0) = f(1)$. Montrer que pour tout entier positif non nul n, il existe $h \in [0, 1 - \frac{1}{n}]$ tel que $f(h) = f(h + \frac{1}{n})$.

Indication : raisonner par l'absurde et calculer alors une somme de terme bien choisis.

Exercice 6.6.20 Soient f et g deux applications continues de $[0, 1]$ dans $[0, 1]$. **On suppose que $g \circ f = f \circ g$**. On veut montrer qu'il existe $x_0 \in [0, 1]$ tel que $f(x_0) = g(x_0)$.

1. *Première méthode : par l'absurde.*
   (a) Traduire mathématiquement l'hypothèse que l'on fait en raisonnant par l'absurde.
   (b) En déduire que quitte à échanger les rôles de f et g, on peut supposer que $\forall x \in [0, 1]\ ,\ f(x) > g(x)$.
   (c) En déduire qu'il existe $\varepsilon > 0$ tel que : $\forall x \in [0, 1]\ ,\ f(x) \geqslant g(x) + \varepsilon$.
   (d) Montrer alors que pour tout entier $n \geqslant 1$, $\forall x \in [0, 1]\ ,\ f^n(x) \geqslant g^n(x) + n\varepsilon$, où f^n désigne $f \circ f \cdots \circ f$ (composée n fois).
   Indication : on pourra commencer par comparer pour $n \in \mathbb{N}^\star$, $f \circ g^n$ et $g^n \circ f$.
   (e) En déduire une contradiction et conclure.
2. *Seconde méthode : par les points fixes.*
   (a) Montrer que l'ensemble $E_f = \{x \in [0, 1]\ ,\ f(x) = x\}$ est non vide.
   (b) Justifier alors l'existence de $\alpha = \inf E_f$ et $\beta = \sup E_f$.
   (c) Montrer qu'en fait, $\alpha = \min E_f$ et $\beta = \max E_f$, c'est-à-dire que $f(\alpha) = \alpha$ et $f(\beta) = \beta$.
   (d) On rappelle que $g \circ f = f \circ g$. Montrer que E_f est stable par g, c'est-à-dire que :
   $$\forall x \in E_f\ ,\ g(x) \in E_f$$
   (e) En déduire les signes de $g(\beta) - f(\beta)$ et de $g(\alpha) - f(\alpha)$.
   (f) Conclure.

Exercice 6.6.21 Soit I un intervalle de $\mathbb{R}$ et $f : I \longrightarrow \mathbb{R}$ une fonction continue.

1. Montrer que si f est strictement monotone, alors elle est injective.
2. On souhaite établir la réciproque du résultat de la question précédente.
   On suppose donc que f est une application continue et injective.
   Soit $(x_0, y_0) \in I^2$ tel que : $x_0 < y_0$. Les réels x_0 et y_0 sont fixés pour toute cette question.
   Soit alors $(x, y) \in I^2$ tel que $x < y$. On appelle g la fonction :

$$g : \begin{array}{ccc} [0,1] & \longrightarrow & \mathbb{R} \\ t & \longmapsto & f\left(y_0 + t(y - y_0)\right) - f\left(x_0 + t(x - x_0)\right) \end{array}$$

   (a) Montrer que : $\forall t \in [0,1]$, $x_0 + t(x - x_0) < y_0 + t(y - y_0)$.
   (b) Montrer que g ne s'annule par $[0,1]$.
   (c) Que peut-on en déduire pour g ?
   (d) En déduire que $f(y) - f(x)$ et $f(y_0) - f(x_0)$ ont le même signe pour tout (x, y) de I^2 tel que $x < y$.
   (e) En déduire que f est strictement monotone.

Exercice 6.6.22 Soit $f : [0,1] \longrightarrow [0,1]$ continue. Démontrer l'équivalence des deux propriétés suivantes :

(i) $f \circ f = f$;
(ii) Il existe deux réels a et b tels que : $0 \leqslant a \leqslant f \leqslant b \leqslant 1$ et $\forall x \in [a, b]$, $f(x) = x$.

Donner un exemple de fonction vérifiant (i) mais telle que $f \notin < \mathrm{Id}_{[0,1]} >$.

Exercice 6.6.23 Soit $f : \mathbb{R} \longrightarrow \mathbb{R}$ continue.

1. On suppose que f admet des limites finies en $+\infty$ et $-\infty$. Montrer que f est bornée. f atteint-elle ses bornes ?
2. On suppose que $\lim\limits_{x \to +\infty} f(x) = \lim\limits_{x \to -\infty} f(x) = +\infty$. Montrer que f est minorée sur $\mathbb{R}$? f admet-elle un minimum ?

Exercice 6.6.24 Soit $f : \mathbb{R}^+ \longrightarrow \mathbb{R}$ continue telle que $\lim\limits_{x \to +\infty} \big[f(x+1) - f(x)\big] = \ell \in \mathbb{R}$. Montrer que $\lim\limits_{x \to +\infty} \dfrac{f(x)}{x} = \ell$.

Exercice 6.6.25 Soit f une application de $\mathbb{R}$ dans $\mathbb{R}$, uniformément continue sur $\mathbb{R}$. Montrer qu'il existe $A, B \in \mathbb{R}$ tels que :

$$\forall x \in \mathbb{R} \ , \ |f(x)| \leqslant A|x| + B$$

Exercice 6.6.26 Soit f une fonction continue sur $[0,1]$ à valeurs réelles. On définit alors :

$$\begin{array}{rcl} \varphi : [0,1] & \longrightarrow & \mathbb{R} \\ x & \longmapsto & \sup\limits_{t\in[0,x]} f(t) \end{array}$$

1. Justifier que l'application φ est bien définie.
2. Étudier les variations de φ.
3. Montrer que φ est continue sur $[0,1]$.

Exercice 6.6.27 La propriété de Borel-Lebesgue et quelques applications simples

1. La propriété de Borel-Lebesgue pour les segments.
   Soit $[a,b]$ un segment de $\mathbb{R}$ (avec $a<b$). On suppose qu'il existe une famille $(]a_i,b_i[)_{i\in I}$ d'intervalles ouverts tels que :
   $$[a,b]\subset\bigcup_{i\in I}]a_i,b_i[$$
   On veut alors prouver qu'il existe J une partie finie de I telle que :
   $$[a,b]\subset\bigcup_{i\in J}]a_i,b_i[$$
   On note $\mathcal{P}_f(I)$ l'ensemble des parties finies de I.
   On considère alors l'ensemble suivant :
   $$A=\left\{x\in[a,b]\ /\ \exists J\in\mathcal{P}_f(I)\ ,\ [a,x]\subset\bigcup_{i\in J}]a_i,b_i[\right\}$$
   (a) Montrer que A admet une borne supérieure.
   (b) Démontrer que $\sup A=\max A$.
   (c) Prouver enfin que $\max A=b$ et conclure.
2. Soit f une application continue sur $[a,b]$ à valeurs dans $\mathbb{K}$. En utilisant la propriété de Borel-Lebesgue, montrer que f est uniformément continue sur $[a,b]$.
3. Soit $f:[a,b]\longrightarrow\mathbb{R}$ une application localement lipschitzienne, c'est-à-dire telle que :
   $$\forall x\in[a,b]\ ,\ \exists r_x>0\ ,\ \exists k_x>0\ ,\ \forall(u,v)\in[a,b]\cap]x-r_x,x+r_x[\ ,\ |f(u)-f(v)|\leqslant k_x|u-v|$$
   Montrer que f est lipschitzienne sur $[a,b]$ en utilisant la propriété de Borel-Lebesgue.
4. Retrouver le résultat de la question précédente, en raisonnant par l'absurde, sans utiliser la propriété de Borel-Lebesgue.

Chapitre 7

Polynômes et fractions rationnelles

Prérequis : dans tout ce chapitre, les notions suivantes sont supposées connues :

- groupes, anneaux, corps et morphismes de groupes ou d'anneaux ;
- espaces vectoriels, sous-espaces vectoriels et applications linéaires ;
- arithmétique dans $\mathbb{Z}$;
- nombres complexes, racines n-ièmes d'un nombre complexe ;
- fonctions polynomiales et opérations sur les fonctions polynomiales.

Aucune connaissance spécifique sur les polynômes n'est supposée connue.

7.1 Ensemble $\mathbb{K}[X]$

Dans tout ce chapitre, $\mathbb{K}$ désigne $\mathbb{R}$ ou $\mathbb{C}$.

7.1.1 Algèbres et morphisme d'algèbres

Définition 7.1.1.1 Soit A un ensemble muni de deux lois de composition internes notées $+$ et $\times$ et d'une multiplication externe sur $\mathbb{K}$, notée $\cdot$. On dit que $(A, +, \times, \cdot)$ est une $\mathbb{K}$-algèbre si :

(i) $(A, +, \times)$ est un anneau ;

(ii) $(A, +, \cdot)$ est un $\mathbb{K}$-espace vectoriel ;

(iii) Pour tout $(x, y) \in A^2$ et tout $\lambda \in \mathbb{K}$, $(\lambda \cdot x) \times y = x \times (\lambda \cdot y) = \lambda \cdot (x \times y)$.

Si de plus $\times$ est commutative, on dit que A est une algèbre commutative.

Exemple 7.1.1.2 On a déjà vu plusieurs exemples dans les chapitres précédents.

- L'exemple le plus simple est $\mathbb{K}$: $\mathbb{K}$ est une $\mathbb{K}$-algèbre commutative (puisque $\mathbb{K}$ est un corps commutatif).
- Si E est un $\mathbb{K}$-espace vectoriel, $(\mathcal{L}_{\mathbb{K}}(E), +, \circ, \cdot)$ est une $\mathbb{K}$-algèbre non commutative en général (c'est-à-dire si E n'est pas réduit à $\{0\}$ et n'est pas une droite vectorielle).
- $(\mathcal{F}(I, \mathbb{K}), +, \times, \cdot)$ est une $\mathbb{K}$-algèbre commutative.
- $(\mathbb{K}^{\mathbb{N}}, +, \times, \cdot)$ est une $\mathbb{K}$-algèbre commutative.

Remarque : *la définition d'une algèbre entraîne que la multiplication $\times$ est une application bilinéaire de $A \times A$ dans A.*

Définition 7.1.1.3 Soit A une $\mathbb{K}$-algèbre et $B \subset A$. On dit que B est une sous-algèbre de A (ou encore une sous-$\mathbb{K}$-algèbre de A) si :

(i) B est un sous-anneau de A ;

(ii) B est un sous-espace vectoriel de A.

Remarque : *comme d'habitude, ici les lois sont sous-entendues. En toute rigueur, il faudrait écrire soit $(A, +, \times, \cdot)$ une $\mathbb{K}$-algèbre. $B \subset A$ est une sous-algèbre de A si $(B, +, \times)$ est un sous-anneau de $(A, +, \times)$ et $(B, +, \cdot)$ est un sous-espace vectoriel de $(A, +, \cdot)$.*

Exemple 7.1.1.4 Dans les chapitres précédents, on a démontré que :

- l'ensemble $\mathcal{S}$ des suites à valeurs dans $\mathbb{K}$ qui convergent est une sous-algèbre de $\mathbb{K}^{\mathbb{N}}$;
- l'ensemble des applications paires de $\mathbb{R}$ dans $\mathbb{R}$ est une sous-algèbre de $\mathcal{F}(\mathbb{R},\mathbb{R})$;
- si E est un $\mathbb{K}$-espace vectoriel, l'ensemble de homothéties de E est une sous-algèbre de $\mathcal{L}(E)$;
- l'ensemble des fonctions continues $\mathbb{R}$ dans $\mathbb{R}$ est une sous-algèbre de $\mathcal{F}(\mathbb{R},\mathbb{R})$.

La proposition suivante donne la caractérisation pratique d'une sous-algèbre (c'est-à-dire ce qu'on utilise dans la pratique).

Proposition 7.1.1.5 *Soit $(A,+,\times,\cdot)$ une $\mathbb{K}$-algèbre. Alors B est une sous-algèbre de A si et seulement si :*

(i) $B \subset A$;

(ii) $1_A \in B$;

(iii) $\forall (x,y) \in B^2$, $\forall (\lambda,\mu) \in \mathbb{K}^2$, $\lambda \cdot x + \mu \cdot y \in B$;

(iv) $\forall (x,y) \in B^2$, $x \times y \in B$.

Preuve :

- Il est évident que si B est une sous-algèbre de A, alors les propriétés $(i),(ii),(iv)$ sont vérifiées car B est un sous-anneau de A et la propriété (iii) est vérifiée car B est un sous-espace vectoriel de A.
- Réciproquement, si B vérifie les propriétés (i), (ii), (iii) et (iv) alors :
  - en choisissant $x = y = 1_A$, $\lambda = 0_{\mathbb{K}}$ et $\mu = 0_{\mathbb{K}}$ dans (iii), on obtient $0_A \in B$. Cette propriété avec (i) et (iii) montre que B est bien un sous-espace vectoriel de A ;
  - en choisissant $\lambda = 1_{\mathbb{K}}$ et $\mu = -1_{\mathbb{K}}$ dans (iii), on obtient $x-y \in B$ pour tout $(x,y) \in B^2$. Ceci avec (i), (ii) et (iv) montre que B est un sous-anneau de A.

⊠

Exercice 7.1.1.6 Soient E un $\mathbb{K}$-espace vectoriel et $f \in \mathcal{L}(E)$. On note :

$$\mathcal{C}(f) = \{g \in \mathcal{L}(E) \ / \ g \circ f = f \circ g\}$$

Montrer que $\mathcal{C}(f)$ est une sous-algèbre de $\mathcal{L}(E)$.

Proposition 7.1.1.7 *Soient $(A, +, \times, \cdot)$ une $\mathbb{K}$-algèbre et B une sous-algèbre de A. Alors $(B, +, \times, \cdot)$ est une $\mathbb{K}$-algèbre.*

Preuve :

C'est évident mais on va néanmoins le justifier.

• Le fait que $(B, +, \times)$ est un sous-anneau de A signifie que les restrictions de $+$ et $\times$ à $B \times B$ sont des applications à valeurs dans B. Autrement dit, $+$ et $\times$ sont bien des lois de composition internes sur B et $(B, +, \times)$ est bien un anneau.

• De même, puisque $(B, +, \cdot)$ est un sous-espace vectoriel de $(A, +, \cdot)$, la restriction de $\cdot$ à $\mathbb{K} \times B$ est à valeurs dans B, c'est-à-dire que $\cdot$ est également une loi de composition externe sur B et $(B, +, \cdot)$ est bien un $\mathbb{K}$-espace vectoriel.

• Enfin, puisque A est une algèbre :

$$\forall (x, y) \in A^2 \ , \ \forall \lambda \in \mathbb{K} \ , \ (\lambda \cdot x) \times y = x \times (\lambda \cdot y) = \lambda \cdot (x \times y)$$

Or, $B \subset A$ donc *a fortiori* :

$$\forall (x, y) \in B^2 \ , \ \forall \lambda \in \mathbb{K} \ , \ (\lambda \cdot x) \times y = x \times (\lambda \cdot y) = \lambda \cdot (x \times y)$$

Ce qui prouve que $(B, +, \times, \cdot)$ est bien une $\mathbb{K}$-algèbre.

$\boxtimes$

Définition 7.1.1.8 Soient $(A, +, \times, \cdot)$ et $(B, \oplus, \otimes, \odot)$ deux $\mathbb{K}$-algèbres. On dit qu'une application $f : A \longrightarrow B$ est un morphisme d'algèbres si :

- f est une application $\mathbb{K}$-linéaire de A dans B ;
- et f est un morphisme d'anneaux de A dans B.

Remarque : *autrement dit, f est un morphisme d'algèbres si :*

(i) $\forall (x, y) \in A^2 \ , \ \forall (\lambda, \mu) \in \mathbb{K}^2 \ , \ f(\lambda \cdot x + \mu \cdot y) = \lambda \odot f(x) \oplus \mu \odot f(y)$;

(ii) $f(1_A) = 1_B$;

(iii) $\forall (x, y) \in A^2 \ , \ f(x \times y) = f(x) \otimes f(y)$.

Exemple 7.1.1.9 Si $\mathcal{S}$ est l'ensemble des suites à valeurs dans $\mathbb{K}$ qui convergent, alors l'application :

$$\varphi : \begin{array}{ccc} \mathcal{S} & \longrightarrow & \mathbb{K} \\ (u_n)_{n\in\mathbb{N}} & \longmapsto & \lim\limits_{n\to+\infty} u_n \end{array}$$

est un morphisme de $\mathbb{K}$-algèbres.

Exemple 7.1.1.10 Les évaluations, c'est-à-dire les applications $e_a : f \longmapsto f(a)$ (pour $a \in I$), sont des morphismes d'algèbres de $\mathcal{F}(I, \mathbb{K})$ dans $\mathbb{K}$.

Exemple 7.1.1.11 En revanche, l'application $I : \mathcal{C}^0([0,1], \mathbb{R}) \longrightarrow \mathbb{R}$ qui à une fonction continue f associe $I(f) = \displaystyle\int_0^1 f(x)\,\mathrm{d}x$ n'est pas un morphisme d'algèbres.

On dispose alors du même vocabulaire que pour les morphismes d'anneaux et les applications linéaires.

Définition 7.1.1.12 Soient A et B deux $\mathbb{K}$-algèbres.

- On dit qu'une application $f : A \longrightarrow B$ est un isomorphisme de $\mathbb{K}$-algèbres (ou un isomorphisme d'algèbres) si f est un morphisme d'algèbres et f est bijective ;
- On dit qu'une application $f : A \longrightarrow A$ est un automorphisme de l'algèbre A si f est un isomorphisme d'algèbres de A dans lui-même.

Exercice 7.1.1.13 L'ensemble $\mathcal{F}(\mathbb{R}, \mathbb{R})$ est une $\mathbb{R}$-algèbre de référence. Pour $a \in \mathbb{R}$, on définit :

$$\psi_a : \begin{array}{ccc} \mathcal{F}(\mathbb{R},\mathbb{R}) & \longrightarrow & \mathcal{F}(\mathbb{R},\mathbb{R}) \\ f & \longmapsto & \psi_a(f) \end{array}$$

où pour $f \in \mathcal{F}(\mathbb{R}, \mathbb{R})$, on a : $\forall x \in \mathbb{R}$, $\psi_a(f)(x) = f(x + a)$. Montrer que ψ_a est un automorphisme de l'algèbre $\mathcal{F}(\mathbb{R}, \mathbb{R})$.

Remarque importante : *Soit A une $\mathbb{K}$-algèbre. On suppose que $A \neq \{0_A\}$, c'est-à-dire que $0_A \neq 1_A$. On considère alors l'application :*

$$\varphi : \begin{array}{ccc} \mathbb{K} & \longrightarrow & A \\ \lambda & \longmapsto & \lambda \cdot 1_A \end{array}$$

Tout d'abord, il est clair que φ est un morphisme de $\mathbb{K}$-algèbres.

De plus, d'après les règles de calculs dans un $\mathbb{K}$-espace vectoriel, puisque $1_A \neq 0_A$, on a :

$$\forall \lambda \in \mathbb{K} \ , \ \Big(\lambda \cdot 1_A = 0 \Longrightarrow \lambda = 0_{\mathbb{K}}\Big)$$

Autrement dit, $\ker(\varphi) = \{0_{\mathbb{K}}\}$, c'est-à-dire φ est injective. Ceci permet d'identifier $\mathbb{K}$ avec $\varphi(\mathbb{K})$, c'est-à-dire d'identifier $\mathbb{K}$ à une sous-algèbre de A en notant 1_A et $1_{\mathbb{K}}$ de la même façon.

7.1.2 Définition d'un polynôme

Définition 7.1.2.1 On appelle polynôme à une indéterminée à coefficients dans $\mathbb{K}$ toute suite $(a_n)_{n\in\mathbb{N}} \in \mathbb{K}^{\mathbb{N}}$ nulle à partir d'un certain rang. On note $\mathbb{K}[X]$ l'ensemble des polynômes à une indéterminée à coefficients dans $\mathbb{K}$.

Remarques :

- *ainsi, par définition, $\mathbb{K}[X] = \{(a_n)_{n\in\mathbb{N}} \in \mathbb{K}^{\mathbb{N}} \ / \ \exists n_0 \in \mathbb{N} \ , \ \forall n \geqslant n_0 \ , \ a_n = 0\}$;*
- *la suite nulle (0) appartient à $\mathbb{K}[X]$: on l'appelle le polynôme nul ;*
- *par définition, deux polynômes $P = (a_n)_{n\in\mathbb{N}}$ et $Q = (b_n)_{n\in\mathbb{N}}$ sont égaux si on a : $\forall n \in \mathbb{N} \ , \ a_n = b_n$;*
- *on verra un peu plus loin pourquoi on utilise la notation $\mathbb{K}[X]$;*
- *cette définition formelle peut sembler « étrange » au premier abord. Si on part de ce que vous avez appris de façon moins formelle, un polynôme est une somme finie $\sum_{k=0}^{n_0} a_k X^k$: cette écriture ou bien la donnée des coefficients, c'est-à-dire les a_k, est la même chose. On retrouve donc qu'un polynôme est une suite finie de coefficients que l'on peut compléter par des zéros pour obtenir une suite $(a_n)_{n\in\mathbb{N}}$ dont tous les termes sont nuls à partir d'un certain rang. On reverra tout cela de façon plus précise et formelle lorsqu'on définira le « X ».*

7.1.3 Opérations usuelles sur les polynômes

Intuitivement, vous avez déjà vu comment on additionne et on multiplie des fonctions polynomiales. Si $f : x \longmapsto \sum_{k=0}^{n} a_k x^k$ et $g : x \longmapsto \sum_{k=0}^{n} b_k x^k$, alors :

$$f + g : x \longmapsto \sum_{k=0}^{n} (a_k + b_k) x^k$$

sauf que le « n » n'est pas forcément le même pour f et pour g (ce sera la notion de degré).

De même, pour tout réel x,

$$(f \times g)(x) = \left(\sum_{i=0}^{n} a_i x^i\right) \times \left(\sum_{j=0}^{n} b_j x^j\right) = \sum_{i=0}^{n}\sum_{j=0}^{n} a_i b_j x^{i+j} = \sum_{k=0}^{2n}\left(\sum_{i+j=k} a_i b_j\right) x^k$$

en regroupant les termes de « même degré » (que nous allons définir proprement plus loin). Ceci nous amène à poser les définitions formelles suivantes.

Définition 7.1.3.1 On définit sur l'ensemble $\mathbb{K}[X]$:

- une première loi de composition interne (une addition), notée $+$, définie par : pour tous polynômes $P = (a_n)_{n\in\mathbb{N}} \in \mathbb{K}[X]$ et $Q = (b_n)_{n\in\mathbb{N}} \in \mathbb{K}[X]$,

$$P + Q = (a_n + b_n)_{n\in\mathbb{N}}$$

- une seconde loi de composition interne, appelée multiplication et notée $\times$, définie par : pour tous polynômes $P = (a_n)_{n\in\mathbb{N}} \in \mathbb{K}[X]$ et $Q = (b_n)_{n\in\mathbb{N}} \in \mathbb{K}[X]$,

$$P \times Q = (c_n)_{n\in\mathbb{N}} \quad \text{avec pour tout } n \in \mathbb{N},\ c_n = \sum_{k=0}^{n} a_k b_{n-k}$$

- une multiplication externe, notée $\cdot$, définie par :

$$\forall \lambda \in \mathbb{K}\ ,\ \forall P = (a_n)_{n\in\mathbb{N}} \in \mathbb{K}[X]\ ,\ \lambda \cdot P = (\lambda \times a_n)_{n\in\mathbb{N}}$$

Remarque : *par définition, l'ensemble $\mathbb{K}[X]$ est inclus dans $\mathbb{K}^{\mathbb{N}}$ et on constate que :*

- *l'addition et la multiplication externe définies sur $\mathbb{K}[X]$ sont les mêmes que sur l'ensemble $\mathbb{K}^{\mathbb{N}}$ (autrement dit, on a simplement restreint à $\mathbb{K}[X]$ l'addition et la multiplication externe sur l'ensemble des suites) ;*

- *en revanche, la multiplication définie dans $\mathbb{K}[X]$ ne correspond pas du tout à la multiplication définie sur l'ensemble $\mathbb{K}^{\mathbb{N}}$. C'est parfaitement logique car on a vu que la « multiplication » revenait à regrouper les termes de « même degré » ce qui visiblement différent de multiplier les termes un à un ;*

- *le produit ainsi défini est aussi appelé produit de Cauchy des suites $(a_n)_{n\in\mathbb{N}}$ et $(b_n)_{n\in\mathbb{N}}$. La notion de produit de Cauchy sera abordée plus en détails dans les cours de mathématiques spéciales 1 (séries) et 2 (séries entières).*

Proposition 7.1.3.2 *$+$, $\times$ sont bien des lois de composition interne sur $\mathbb{K}[X]$ et $\cdot$ est bien une loi de composition externe sur $\mathbb{K}[X]$.*

Preuve :

Soient $P = (a_n)_{n\in\mathbb{N}}$ et $Q = (b_n)_{n\in\mathbb{N}}$ deux polynômes et $\lambda \in \mathbb{K}$. On doit justifier que $P + Q$, $P \times Q$ et $\lambda \cdot P$ sont bien des polynômes.
Par définition, il existe $n_1, n_2 \in \mathbb{N}$ tels que :

$$\forall n \geqslant n_1 \ , \ a_n = 0 \quad \text{et} \quad \forall n \geqslant n_2 \ , \ b_n = 0$$

• Pour commencer, en posant $n_0 = \max(n_1, n_2)$, on a :

$$\forall n \geqslant n_0 \ , \ a_n + b_n = 0$$

Par suite, $P + Q \in \mathbb{K}[X]$.

• Ensuite, $\forall n \geqslant n_1 \ , \ \lambda \times a_n = 0$ donc $\lambda \cdot P \in \mathbb{K}[X]$.

• Enfin, montrons que pour tout entier $n \geqslant n_1 + n_2$, $c_n = \displaystyle\sum_{k=0}^{n} a_k b_{n-k} = 0$.
On a deux cas possibles :

∗ si $0 \leqslant k \leqslant n_1$, alors $n - k \geqslant n_1 + n_2 - n_1 = n_2$ et $b_{n-k} = 0$. A fortiori, $a_k b_{n-k} = 0$;

∗ si $n_1 < k$, alors $a_k = 0$ et *a fortiori*, $a_k b_{n-k} = 0$.

Ainsi, $\forall k \in [\![0, n]\!] \ , \ a_k b_{n-k} = 0$ et donc $c_n = 0$.
Ce qui prouve que $c_n = \displaystyle\sum_{k=0}^{n} a_k b_{n-k} = 0$ pour $n \geqslant n_1 + n_2$ et donc $P \times Q$ est bien un polynôme.

⊠

Remarque : *dans la démonstration précédente, les choix de $n \geqslant max(n_1, n_2)$ ou bien $n \geqslant n_1 + n_2$ sont parfaitement logiques. En effet, cela correspond aux propriétés du degré (que l'on va formaliser un peu plus loin) : si P est de degré $n_1 - 1$ et Q est de degré $n_2 - 1$, alors $P \times Q$ est de degré $n_1 + n_2 - 2$. Vous pouvez d'ailleurs remarquer que dans la preuve, on pouvait aussi choisir $n \geqslant n_1 + n_2 - 1$ dans le cas du produit.*

On peut maintenant énoncer le théorème fondamental sur la structure de l'ensemble $\mathbb{K}[X]$. La démonstration est purement calculatoire et ne présente aucune difficulté théorique. Elle peut être omise en première lecture. Autrement dit, il n'est pas nécessaire de maîtriser cette démonstration mais c'est un bon exercice de manipulation des sommes.

Théorème 7.1.3.3 $(\mathbb{K}[X], +, \times, \cdot)$ *est une* $\mathbb{K}$*-algèbre commutative, appelée algèbre des polynômes à une indéterminée.*

Preuve :

• Pour commencer, on a déjà remarqué de $\mathbb{K}[X] \subset \mathbb{K}^{\mathbb{N}}$ et que $(\mathbb{K}^{\mathbb{N}}, +, \cdot)$ est un $\mathbb{K}$-espace vectoriel. De plus,

- $0_{\mathbb{K}^{\mathbb{N}}} \in \mathbb{K}[X]$ (tous les termes sont nuls à partir du rang $n = 0$) ;
- $\mathbb{K}[X]$ est stable par $+$ et $\cdot$ (proposition précédente).

Ceci prouve dans un premier temps que $(\mathbb{K}[X], +, \cdot)$ est un sous-espace vectoriel de $(\mathbb{K}^{\mathbb{N}}, +, \cdot)$: c'est donc bien un $\mathbb{K}$-espace vectoriel.

• Montrons que $(\mathbb{K}[X], +, \times)$ est un anneau commutatif.

- $+$ et $\times$ sont des lois de composition internes sur $\mathbb{K}[X]$ (proposition précédente) ;
- $(\mathbb{K}[X], +)$ est un groupe abélien (car $(\mathbb{K}[X], +, \cdot)$ est un espace vectoriel) ;
- $\times$ est clairement commutative car si $P = (a_n)_{n\in\mathbb{N}} \in \mathbb{K}[X]$ et $Q = (b_n)_{n\in\mathbb{N}} \in \mathbb{K}[X]$, alors :

$$P \times Q = (c_n)_{n\in\mathbb{N}} \quad \text{et} \quad Q \times P = (d_n)_{n\in\mathbb{N}}$$

avec, par définition, pour tout entier $n \in \mathbb{N}$:

$$c_n = \sum_{k=0}^{n} a_k b_{n-k} \quad ; \quad d_n = \sum_{k=0}^{n} b_k a_{n-k}$$

Le changement d'indice $j = n-k$ montre directement que $c_n = d_n$ pour tout entier n, c'est-à-dire $(c_n)_{n\in\mathbb{N}} = (d_n)_{n\in\mathbb{N}}$, soit encore $P \times Q = Q \times P$.

- Montrons qu'il existe un élément neutre pour $\times$ (dans $\mathbb{K}[X]$).
  Notons $1_{\mathbb{K}[X]} = (\delta_0(n))_{n\in\mathbb{N}}$ (c'est-à-dire la suite dont le terme d'indice 0 vaut 1 et tous les suivants sont nuls).
  - ▷ Par définition, $1_{\mathbb{K}[X]} \in \mathbb{K}[X]$.
  - ▷ Soit $P = (a_n)_{n\in\mathbb{N}} \in \mathbb{K}[X]$. On note $1_{\mathbb{K}[X]} \times P = (c_n)_{n\in\mathbb{N}}$. Alors :

$$\forall n \in \mathbb{N}\ ,\ c_n = \sum_{k=0}^{n} \delta_0(k) a_{n-k} = a_n$$

Ainsi $(c_n)_{n\in\mathbb{N}} = (a_n)_{n\in\mathbb{N}}$, c'est-à-dire $1_{\mathbb{K}[X]} \times P = P$. Or, $\times$ est commutative donc $1_{\mathbb{K}[X]} \times P = P \times 1_{\mathbb{K}[X]} = P$.

Ce qui prouve que $1_{\mathbb{K}[X]}$ est un élément neutre pour $\times$.

∗ Montrons que $\times$ est associative.

Soient $P = (a_n)_{n\in\mathbb{N}}$, $Q = (b_n)_{n\in\mathbb{N}}$ et $R = (c_n)_{n\in\mathbb{N}}$ trois éléments de $\mathbb{K}[X]$. On note :

$$P \times Q = (u_n)_{n\in\mathbb{N}} \ ; \ (P \times Q) \times R = (v_n)_{n\in\mathbb{N}}$$

$$Q \times R = (w_n)_{n\in\mathbb{N}} \ ; \ P \times (Q \times R) = (t_n)_{n\in\mathbb{N}}$$

Soit $n \in \mathbb{N}$.

$$t_n = \sum_{k=0}^{n} a_k w_{n-k} = \sum_{k=0}^{n} a_k \left(\sum_{j=0}^{n-k} b_j c_{n-k-j} \right) = \sum_{k=0}^{n} \sum_{j=0}^{n-k} a_k b_j c_{n-k-j}$$

soit encore

$$t_n = \sum_{k=0}^{n} \sum_{j=0}^{n-k} a_k b_{n-k-j} c_j$$

En réalité, cette somme double porte sur les indices j, k dans $[\![0, n]\!]$ tels que $k + j \leqslant n$. En changeant l'ordre de sommation, on obtient :

$$t_n = \sum_{j=0}^{n} \sum_{k=0}^{n-j} a_k b_{n-k-j} c_j = \sum_{j=0}^{n} \left(\sum_{k=0}^{n-j} a_k b_{n-j-k} \right) c_j = \sum_{j=0}^{n} u_{n-j} c_j$$

soit encore, en posant $l = n - j$,

$$t_n = \sum_{l=0}^{n} u_l c_{n-l} = v_n$$

Ce qui prouve que $(t_n)_{n\in\mathbb{N}} = (v_n)_{n\in\mathbb{N}}$, c'est-à-dire :

$$(P \times Q) \times R = P \times (Q \times R)$$

Ainsi, $\times$ est associative.

∗ Il reste alors à prouver la distributivité de $\times$ par rapport à $+$ (à gauche uniquement car $\times$ est commutative).

Soient $P = (a_n)_{n\in\mathbb{N}}$, $Q = (b_n)_{n\in\mathbb{N}}$ et $R = (c_n)_{n\in\mathbb{N}}$ trois éléments de $\mathbb{K}[X]$.

On a alors :

$$\begin{aligned}(P+Q)\times R &= \left(\sum_{k=0}^{n}(a_k+b_k)c_{n-k}\right)_{n\in\mathbb{N}}\\ &= \left(\sum_{k=0}^{n}a_kc_{n-k}+\sum_{k=0}^{n}b_kc_{n-k}\right)_{n\in\mathbb{N}}\\ &= \left(\sum_{k=0}^{n}a_kc_{n-k}\right)_{n\in\mathbb{N}}+\left(\sum_{k=0}^{n}b_kc_{n-k}\right)_{n\in\mathbb{N}}\\ &= P\times R+Q\times R\end{aligned}$$

Ainsi, $\times$ est distributive par rapport à $+$ à gauche. Or, $\times$ est commutative donc $\times$ est également distributive par rapport à $+$ à droite.

• Il reste enfin à montrer que :

$$\forall(P,Q)\in\mathbb{K}[X]^2\ ,\ \forall\lambda\in\mathbb{K}\ ,\ (\lambda\cdot P)\times Q=P\times(\lambda\cdot Q)=\lambda\cdot(P\times Q)$$

Soient $P=(a_n)_{n\in\mathbb{N}}$, $Q=(b_n)_{n\in\mathbb{N}}$ deux éléments de $\mathbb{K}[X]$ et $\lambda\in\mathbb{K}$. Par définition, on a :

$$\begin{aligned}(\lambda\cdot P)\times Q &= \left(\sum_{k=0}^{n}(\lambda a_k)b_{n-k}\right)_{n\in\mathbb{N}}\\ &= \left(\sum_{k=0}^{n}a_k(\lambda b_{n-k})\right)_{n\in\mathbb{N}}\\ &= P\times(\lambda\cdot Q)\\ &= \left(\lambda\sum_{k=0}^{n}a_kb_{n-k}\right)_{n\in\mathbb{N}}\\ &= \lambda\cdot(P\times Q)\end{aligned}$$

Ceci prouve donc que $(\mathbb{K}[X],+,\times,\cdot)$ est une $\mathbb{K}$-algèbre commutative. ⊠

Remarques :

- *le neutre pour l'addition est le polynôme nul (suite constante égale à 0) ;*
- *le neutre pour la multiplication est le polynôme $(\delta_0(n))_{n\in\mathbb{N}}$ avec $\delta_0(n)=0$ si $n\neq 0$ et $\delta_0(0)=1$, ou de façon moins formelle, $(1,0,\cdots,0\cdots)$. En identifiant $\mathbb{K}$ et $\{\lambda(\delta_0(n))_{n\in\mathbb{N}}\ ,\ \lambda\in\mathbb{K}\}$, le neutre pour la multiplication est donc $1_{\mathbb{K}}$. On dit que c'est le polynôme constant égal à 1.*

On peut maintenant justifier l'écriture $\mathbb{K}[X]$.

Définition 7.1.3.4 On note $X = (\delta_1(n))_{n\in\mathbb{N}}$ avec $\delta_1(n) = 1$ si $n = 1$ et 0 sinon. On appelle X l'indéterminée.

Remarque : *de façon moins formelle,* $X = (0, 1, 0, 0, \cdots, 0\cdots)$ *ce qui correspond bien à l'écriture que l'on verra après, c'est-à-dire* $X = 0 \times X^0 + 1 \times X^1 + 0 \times X^2 + \cdots$.

Proposition 7.1.3.5 *Pour tout entier* $k \in \mathbb{N}$, $X^k = (\delta_k(n))_{n\in\mathbb{N}}$, *c'est-à-dire* X^k *est la suite dont tous les termes sont nuls sauf celui d'indice* k *qui vaut* 1.

Preuve :

On procède par récurrence.

Initialisation :

Par définition, $X^0 = 1_{\mathbb{K}[X]}$ et on a vu que $1_{\mathbb{K}[X]} = (\delta_0(n))_{n\in\mathbb{N}}$. La propriété est donc vraie au rang $k = 0$.

Hérédité :

Soit $k \in \mathbb{N}$. On suppose que $X^k = (\delta_k(n))_{n\in\mathbb{N}}$ et on montre alors que $X^{k+1} = (\delta_{k+1}(n))_{n\in\mathbb{N}}$.

$$X^{k+1} = X \times X^k = (\delta_1(n))_{n\in\mathbb{N}} \times (\delta_k(n))_{n\in\mathbb{N}}$$

Or, par définition de $\times$,

$$\begin{aligned}(\delta_1(n))_{n\in\mathbb{N}} \times (\delta_k(n))_{n\in\mathbb{N}} &= \left(\sum_{j=0}^{n} \delta_1(j)\delta_k(n-j)\right)_{n\in\mathbb{N}} \\ &= (\delta_k(n-1))_{n\in\mathbb{N}} \\ &= (\delta_{k+1}(n))_{n\in\mathbb{N}}\end{aligned}$$

Ce qui prouve que la propriété est vraie au rang $k + 1$ et achève la récurrence.

⊠

Corollaire 7.1.3.6 *Pour tout* $(n, p) \in \mathbb{N}^2$, $X^n \times X^p = X^{n+p}$.

Preuve :

| À nouveau, il suffit de faire une simple vérification par le calcul. ⊠

Notation

Soit $P \in \mathbb{K}[X]$. Alors $P = (a_n)_{n\in\mathbb{N}}$ et il existe $N \in \mathbb{N}$ tel que : $\forall n \geqslant N$, $a_n = 0$. On a alors :

$$(a_n)_{n\in\mathbb{N}} = \sum_{k=0}^{N} a_k(\delta_k(n))_{n\in\mathbb{N}} = \sum_{k=0}^{N} a_k X^k$$

On écrira donc un polynôme P sous l'une des formes suivantes :

- $P = \sum_{k=0}^{N} a_k X^k$ où $N \in \mathbb{N}$;
- ou encore $P = \sum a_n X^n$;
- ou encore $\sum_{n=0}^{+\infty} a_n X^n$ mais dans ce cas, on doit préciser que tous les termes de la suite $(a_n)_{n\in\mathbb{N}}$ sont nuls à partir d'un certain rang.

Ainsi, tout polynôme P s'écrit de façon unique sous la forme : $P = \sum_{n=0}^{+\infty} a_n X^n$, où les $a_n \in \mathbb{K}$ et sont tous nuls à partir d'un certain rang.

Dans la pratique, on utilise plutôt l'écriture suivante :

$$P \in \mathbb{K}[X] \iff \exists N \in \mathbb{N} \text{ , } \exists (a_k)_{0\leqslant k\leqslant N} \in \mathbb{K}^{N+1} \text{ , } P = \sum_{k=0}^{N} a_k X^k$$

Définition 7.1.3.7 On appelle monôme tout polynôme P de la forme $P = a_n X^n$ avec $n \in \mathbb{N}$ et $a_n \in \mathbb{K}$.

Définition 7.1.3.8 Soit $P = \sum a_n X^n$ un polynôme. Pour $n \in \mathbb{N}$, on dit que a_n est le coefficient de X^n dans P et le monôme $a_n X^n$ est appelé le terme de degré n de P.

7.1.4 Dérivation sur l'ensemble des polynômes

Définition 7.1.4.1 Soit P un polynôme, $P = \sum_{n=0}^{+\infty} a_n X^n$ avec $(a_n)_{n\in\mathbb{N}}$ une suite dont tous les termes sont nuls à partir d'un certain rang. On définit le polynôme dérivé de P, noté P' ou encore $D(P)$, par :

$$P' = D(P) = \sum_{n=1}^{+\infty} n a_n X^{n-1} = \sum_{n=0}^{+\infty} (n+1) a_{n+1} X^n$$

⚠ **Attention :** à nouveau, notez bien qu'il s'agit en réalité d'une somme finie !

Remarques :

- *puisqu'il s'agit d'un polynôme, $D(P)$ est une définition. Il n'y a aucun sens à justifier l'existence de $D(P)$! Il ne faut pas confondre avec une fonction polynôme où, dans ce cas, il y a un sens à justifier l'existence de la fonction dérivée ;*
- *dans la pratique, on rédigera plutôt sous la forme suivante pour éviter d'introduire des sommes « infinies » : soit $P \in \mathbb{K}[X]$, il existe $N \in \mathbb{N}$ et $(a_n)_{0\leqslant n\leqslant N} \in \mathbb{K}^{N+1}$ tels que : $P = \sum_{n=0}^{N} a_n X^n$. Alors :*

  * *si $N = 0$, $D(P) = 0$;*
  * *si $N \geqslant 1$, $D(P) = \sum_{n=1}^{N} n a_n X^{n-1} = \sum_{n=0}^{N-1} (n+1) a_{n+1} X^n$.*

  En convenant qu'une somme vide vaut toujours 0, on peut alors simplement écrire $D(P) = \sum_{n=0}^{N-1} (n+1) a_{n+1} X^n$, sans avoir à distinguer les cas $N = 0$ et $N \geqslant 1$.

Exemple 7.1.4.2 Le calcul direct montre que :

$$\forall n \in \mathbb{N}^\star \ , \ D(X^n) = n X^{n-1} \quad \text{et} \quad \forall \lambda \in \mathbb{K} \ , \ D(\lambda) = 0$$

Remarque : *on peut d'ailleurs remarquer que la formule précédente reste valable pour $n = 0$ mais il faudrait théoriquement pour cela donner un sens à X^{-1}.*

Proposition 7.1.4.3 *L'application dérivation $D : \mathbb{K}[X] \longrightarrow \mathbb{K}[X]$ est une application linéaire vérifiant :*

$$\forall P, Q \in \mathbb{K}[X] \ , \ D(PQ) = D(P)Q + PD(Q)$$

Preuve :

- La linéarité est évidente. La rédaction précise est laissée en exercice.
- Pour la règle avec le produit, on va procéder en plusieurs étapes.
  - ∗ On commence par montrer que la propriété est vraie pour les monômes.
    Soient $\in \mathbb{N}^\star$ et $p \in \mathbb{N}^\star$. On a alors :
    $$\begin{aligned} D(X^n \times X^p) &= D(X^{n+p}) \\ &= (n+p)X^{n+p-1} \\ &= nX^{n-1} \times X^p + X^n \times pX^{p-1} \\ &= D(X^n)X^p + X^n D(X^p) \end{aligned}$$
    Lorsque $n = 0$ (respectivement $p = 0$), la formule est évidente puisque $D(X^n) = 0$ (respectivement $D(X^p) = 0$).
  - ∗ Ensuite, on étend le résultat aux polynômes par bilinéarité du produit et linéarité de la dérivation.
    Soient $P \in \mathbb{K}[X]$ et $Q \in \mathbb{K}[X]$. Par définition, il existe $n \in \mathbb{N}$, $p \in \mathbb{N}$, $(a_k)_{0\leqslant k\leqslant n} \in \mathbb{K}^{n+1}$ et $(b_k)_{0\leqslant k\leqslant p} \in \mathbb{K}^{p+1}$ tels que :
    $$P = \sum_{k=0}^{n} a_k X^k \quad \text{et} \quad Q = \sum_{j=0}^{p} b_j X^j$$
    Alors, par bilinéarité du produit : $P \times Q = \sum_{k=0}^{n}\sum_{j=0}^{p} a_k b_j X^{k+j}$.
    Et donc, par linéarité de la dérivation,
    $$D(P \times Q) = \sum_{k=0}^{n}\sum_{j=0}^{p} a_k b_j D(X^{k+j}) = \sum_{k=0}^{n}\sum_{j=0}^{p} a_k b_j (k+j) X^{k+j-1}$$
    soit encore :
    $$D(P \times Q) = \sum_{k=0}^{n}\sum_{j=0}^{p} k a_k X^{k-1} \times b_j X^j + \sum_{k=0}^{n}\sum_{j=0}^{p} a_k X^k \times j b_j X^{j-1}$$

Or,

$$\begin{aligned}\sum_{k=0}^{n}\sum_{j=0}^{p} ka_kX^{k-1}\times b_jX^j &= \left(\sum_{k=0}^{n} ka_kX^{k-1}\right)\times\left(\sum_{j=0}^{p} b_jX^j\right)\\ &= D(P)\times Q\end{aligned}$$

et de même,

$$\begin{aligned}\sum_{k=0}^{n}\sum_{j=0}^{p} a_kX^k\times jb_jX^{j-1} &= \left(\sum_{k=0}^{n} a_kX^k\right)\times\left(\sum_{j=0}^{p} jb_jX^{j-1}\right)\\ &= P\times D(Q)\end{aligned}$$

D'où l'on obtient bien $D(P\times Q)=D(P)\times Q+P\times D(Q)$. ⊠

Remarque : *on reverra dans le cours de mathématiques supérieures 2 que les arguments en fait utilisés ici sont les suivants :*

- *les applications :*

$$\phi : \begin{array}{ccc}\mathbb{K}[X]\times\mathbb{K}[X] & \longrightarrow & \mathbb{K}[X]\\ (P,Q) & \longmapsto & D(PQ)\end{array} \quad \text{et } \psi : \begin{array}{ccc}\mathbb{K}[X]\times\mathbb{K}[X] & \longrightarrow & \mathbb{K}[X]\\ (P,Q) & \longmapsto & D(P)Q+PD(Q)\end{array}$$

  sont bilinéaires ;
- *la famille $(X^k)_{k\in\mathbb{N}}$ est une base de $\mathbb{K}[X]$;*
- *les applications ϕ et ψ sont donc égales si et seulement si :*

$$\forall (i,j)\in\mathbb{N}^2\ ,\ \phi(X^i,X^j)=\psi(X^i,X^j)$$

Définition 7.1.4.4 Soit P un polynôme. On définit les polynômes dérivés successifs de P par la relation de récurrence :

$$P^{(0)}=P \quad \text{et} \quad \forall n\in\mathbb{N}\ ,\ P^{(n+1)}=D(P^{(n)})$$

Remarque : *autrement dit, pour $n\in\mathbb{N}$, $P^{(n)}=D^n(P)$ où $D^n=\underbrace{D\circ D\circ\cdots\circ D}_{n\ fois}$.*

Exercice 7.1.4.5 (Résultat à connaître) Soit $n\in\mathbb{N}$. Montrer que :

$$\forall k\in\mathbb{N}\ ,\ D^k(X^n)=k!\binom{n}{k}X^{n-k}$$

avec la convention que $\binom{n}{k}=0$ si $k>n$.

7.2 Degré d'un polynôme

7.2.1 Définition

Définition 7.2.1.1 Soit $P = \sum a_k X^k \in \mathbb{K}[X]$. On définit le degré de P, noté $\deg(P)$ (ou aussi d^oP) par :

- si $P = 0$, on pose $\deg(P) = -\infty$;
- si $P \neq 0$, on pose $\deg(P) = \max\{k \in \mathbb{N} \ , \ a_k \neq 0\}$.

Remarque : *le degré est bien défini car :*

- *d'une part, le polynôme P s'écrit de façon unique $P = \sum_{k=0}^{+\infty} a_k X^k$ avec les termes de la suite $(a_n)_{n\in\mathbb{N}}$ tous nuls à partir d'un certain rang ;*
- *et d'autre part, par définition, les coefficients sont tous nuls à partir d'un certain rang donc l'ensemble $\{k \in \mathbb{N} \ , \ a_k \neq 0\}$ est majoré dans $\mathbb{N}$ et non vide lorsque $P \neq 0$.*

Proposition 7.2.1.2 *Soient $P = \sum a_k X^k$ un polynôme non nul et $n = \deg(P) \in \mathbb{N}$. Alors :*

$$a_n \neq 0 \ \text{ et } \forall k \in \mathbb{N} \ , \ (k > n \Longrightarrow a_k = 0)$$

Preuve :

| C'est évident ! C'est la définition du plus grand élément.

⊠

Exemple 7.2.1.3 Les exemples suivants sont simples mais importants :

$$\deg(P) = -\infty \iff P = 0 \quad ; \quad \deg(P) = 0 \iff P = \lambda \in \mathbb{K}^\star$$

Définition 7.2.1.4 Soient $P = \sum a_k X^k$ un polynôme non nul et $n = \deg(P) \in \mathbb{N}$.

- Le coefficient a_n est appelé le coefficient dominant de P ;
- on dit que P est unitaire (ou normalisé) si son coefficient dominant vaut 1 ;
- le coefficient a_0 est appelé le coefficient constant de P.

7.2.2 Propriétés du degré

Proposition 7.2.2.1 *L'application* $\deg : \mathbb{K}[X] \longrightarrow \mathbb{N} \cup \{-\infty\}$ *vérifie les propriétés suivantes :*

(i) *Pour tout* $(P, Q) \in \mathbb{K}[X]^2$, $\deg(P+Q) \leqslant \max(\deg(P), \deg(Q))$.
De plus, si $\deg(P) \neq \deg(Q)$, *il y a égalité :* $\deg(P+Q) = \max(\deg(P), \deg(Q))$

(ii) $\forall (P, Q) \in \mathbb{K}[X]^2$, $\deg(PQ) = \deg(P) + \deg(Q)$.

(iii) *Pour tout* $P \in \mathbb{K}[X]$,

$$\deg(P') = \begin{cases} \deg(P) - 1 & si\ \deg(P) \geqslant 1 \\ -\infty & si\ \deg(P) \leqslant 0 \end{cases}$$

Preuve :

• Montrons (i) et (ii).

Tout d'abord, on remarque que si $P = 0$ ou $Q = 0$, les propriétés (i) et (ii) sont évidentes (avec la règle de calcul $n + (-\infty) = (-\infty) + n = -\infty$ pour tout $n \in \mathbb{N} \cup \{-\infty\}$).

On suppose à présent $P \neq 0$ et $Q \neq 0$. On pose alors $n = \deg(P)$ et $p = \deg(Q)$ (et on a donc $n \in \mathbb{N}$ et $p \in \mathbb{N}$). Alors :

$$P = \sum_{k=0}^{n} a_k X^k \quad \text{et} \quad Q = \sum_{k=0}^{p} b_k X^k$$

où $(a_k)_{k\in\mathbb{N}}, (b_k)_{k\in\mathbb{N}} \in \mathbb{K}^{\mathbb{N}}$ vérifient $a_n \neq 0$, $b_p \neq 0$ et :

$$\forall k > n\ ,\ a_k = 0 \quad \text{et} \quad \forall k > p\ ,\ b_k = 0$$

$*$ D'une part, en reprenant la démonstration de la proposition 7.1.3.2 (c'est-à-dire du fait que $+$ et $\times$ sont des lois de composition internes dans $\mathbb{K}[X]$), on a : $\forall k > \max(n, p)\ ,\ a_k + b_k = 0$. Par suite,

$$\deg(P+Q) \leqslant \max(n, p) = \max(\deg(P), \deg(Q))$$

Et en posant $P \times Q = \sum c_k X^k$,

$$\forall k > n + p\ ,\ c_k = \sum_{i=0}^{k} a_i b_{k-i} = 0 \ \text{ donc } \ \deg(P \times Q) \leqslant n + p$$

∗ D'autre part,

$$c_{n+p} = \sum_{i=0}^{n+p} a_i b_{n+p-i} = \sum_{i=0}^{n} a_i b_{n+p-i} = a_n b_p$$

puisque $a_i = 0$ pour $i > n$ et de même, $b_{n+p-i} = 0$ pour $n + p - i > p$, c'est-à-dire $i < n$. Par suite, $c_{n+p} \neq 0$ et donc $\deg(P \times Q) \geqslant n + p$. Ce qui prouve que $\deg(P \times Q) = \deg(P) + \deg(Q)$.

∗ Si $\deg(P) \neq \deg(Q)$, quitte à renommer les polynômes, on peut supposer que $\deg(Q) < \deg(P)$. Alors $a_n + b_n = a_n + 0 = a_n \neq 0$. Par conséquent, $\deg(P + Q) \geqslant n$, c'est-à-dire $\deg(P + Q) \geqslant \max(\deg(P), \deg(Q))$ et on obtient donc $\deg(P + Q) = \max(\deg(P), \deg(Q))$.

• La propriété (*iii*) est évidente par définition du degré et de P'.

⊠

7.2.3 Conséquences fondamentales

Proposition 7.2.3.1 *L'anneau $\mathbb{K}[X]$ est un anneau intègre, c'est-à-dire :*

$$\forall P, Q \in \mathbb{K}[X] \ , \ (\ PQ = 0 \Longrightarrow P = 0 \ \textit{ou} \ Q = 0\ )$$

Preuve :

En effet, soient P et Q deux polynômes. Par contraposée, si $P \neq 0$ et $Q \neq 0$ alors :

$$\deg(PQ) = \deg(P) + \deg(Q) \geqslant 0$$

Par suite, $PQ \neq 0$.

⊠

Proposition 7.2.3.2 *Les éléments inversibles de l'anneau $\mathbb{K}[X]$ sont les polynômes constants non nuls, c'est-à-dire $\mathbb{K}^\star$.*

Preuve :

• Il est clair que les éléments de $\mathbb{K}^\star$ sont inversibles pour $\times$ dans $\mathbb{K}[X]$.

• Réciproquement, si $P \in \mathbb{K}[X]$ est inversible, alors il existe $Q \in \mathbb{K}[X]$ tel que $PQ = QP = 1$. En prenant les degrés, il vient : $\deg P + \deg Q = 0$, c'est-à-dire $\deg P = \deg Q = 0$. Par suite, $P \in \mathbb{K}^\star$.

⊠

Proposition 7.2.3.3 *Pour tout entier $n \in \mathbb{N}$, l'ensemble :*

$$\mathbb{K}_n[X] = \{P \in \mathbb{K}[X] \ / \ \deg(P) \leqslant n\}$$

est un sous-espace vectoriel de $\mathbb{K}[X]$.

Preuve :

Soit $n \in \mathbb{N}$. Montrons que $\mathbb{K}_n[X]$ est un sous-espace vectoriel de $\mathbb{K}[X]$.

- Tout d'abord, $0 \in \mathbb{K}_n[X]$ puisque $\deg(0) = -\infty \leqslant n$.
- Ensuite, soient $P, Q \in \mathbb{K}_n[X]$. Alors :

  $$\deg(P+Q) \leqslant \max(\deg(P), \deg(Q)) \leqslant n$$

  donc $P + Q \in \mathbb{K}_n[X]$.
- Enfin, soient $P \in \mathbb{K}_n[X]$ et $\lambda \in \mathbb{K}$. Alors :

  $$\deg(\lambda \cdot P) = \deg(\lambda) + \deg(P) \leqslant 0 + n \leqslant n$$

  Par suite, $\lambda \cdot P \in \mathbb{K}_n[X]$.

Ce qui prouve que $\mathbb{K}_n[X]$ est bien un sous-espace vectoriel de $\mathbb{K}[X]$. ⊠

⚠ **Attention :** $\mathbb{K}_n[X]$ n'est pas un sous-anneau de $\mathbb{K}[X]$, sauf si $n = 0$!

7.3 Arithmétique dans $\mathbb{K}[X]$

Dans ce paragraphe, on va voir que les propriétés d'arithmétique dans $\mathbb{Z}$ restent valables dans $\mathbb{K}[X]$: il faut simplement donner les définitions appropriées dans $\mathbb{K}[X]$.

7.3.1 Divisibilité dans $\mathbb{K}[X]$

Définition 7.3.1.1 Soient A et B deux polynômes. On dit que A divise B (ou encore que B est un multiple de A) s'il existe $Q \in \mathbb{K}[X]$ tel que $B = QA$. On note alors $A|B$.

Remarque : *c'est la même définition que dans $\mathbb{Z}$.*

Notation

Dans $\mathbb{Z}$, on a noté $n\mathbb{Z} = \{kn\ ,\ k \in \mathbb{Z}\}$. De façon analogue, si $A \in \mathbb{K}[X]$, l'ensemble des multiples de A sera noté $A\mathbb{K}[X]$. Ainsi,

$$A\mathbb{K}[X] = \{QA\ ,\ Q \in \mathbb{K}[X]\}$$

Remarque : *on peut remarquer que :*

(i) $\forall A \in \mathbb{K}[X]\ ,\ \forall \lambda \in \mathbb{K}^\star,\ \lambda | A$ *;*

(ii) $\forall A \in \mathbb{K}[X]\ ,\ A|0$ *et* $A|A$ *;*

(iii) $\forall A \in \mathbb{K}[X]\ ,\ (\ 0|A \iff A = 0\ )$ *;*

(iv) Pour $A, B, C \in \mathbb{K}[X]$*, si* $A|B$ *et* $A|C$*, alors pour tout* $P, Q \in \mathbb{K}[X]$*,* $A|(PB+QC)$ *;*

(v) Pour tout $(A, B) \in \mathbb{K}[X]^2$*,* $A|B \iff B\mathbb{K}[X] \subset A\mathbb{K}[X]$*.*

Exemple 7.3.1.2 $X - i$ divise $X^2 + 1$ dans $\mathbb{C}[X]$ mais pas dans $\mathbb{R}[X]$.

Exemple 7.3.1.3 Soit $n \in \mathbb{N}^\star$. Alors $A = X - 1$ divise $B = X^n - 1$. En effet,

$$X^n - 1 = \left(\sum_{k=0}^{n-1} X^k\right) \times (X - 1)$$

Exemple 7.3.1.4 $X^2 + X + 1$ divise $X^6 - 1$ car on peut vérifier que :

$$X^6 - 1 = (X^2 + X + 1)(X^4 - X^3 + X - 1)$$

Remarques :

- *tout comme dans $\mathbb{Z}$, la relation $|$ dans $\mathbb{K}[X]$ est réflexive, transitive mais n'est pas antisymétrique ;*
- *pour $a, b \in \mathbb{Z}$, on a vu que $(a|b$ et $b|a) \iff |b| = |a| \iff b = \pm a$. En fait, cela se traduit par $b = u \times a$ avec $u \in \{-1, 1\}$. L'ensemble $\{-1, 1\}$ est l'ensemble des éléments inversibles de l'anneau $\mathbb{Z}$ (on dit aussi que ce sont les unités de $\mathbb{Z}$). Or, dans $\mathbb{K}[X]$, on a vu que les unités sont les $\lambda \in \mathbb{K}^\star$. On va donc retrouver une version analogue du résultat précédent.*

Proposition 7.3.1.5 *Soit* $(A, B) \in \mathbb{K}[X]^2$*. Alors,*

$$(A|B \text{ et } B|A) \iff \exists \lambda \in \mathbb{K}^\star \ , \ B = \lambda A$$

Preuve :

• L'implication $\Longleftarrow$ est claire.

• Montrons à présent $\Longrightarrow$.
On suppose que $A|B$ et $B|A$. Par définition, il existe donc $C, D \in \mathbb{K}[X]$ tels que :

$$A = BC \quad \text{et} \quad B = AD$$

Il s'ensuit que $A = (AD)C = A(DC)$, soit encore $A(1 - DC) = 0$. L'anneau $\mathbb{K}[X]$ étant intègre, on en déduit qu'il y a deux cas.

∗ Premier cas : $A = 0$.
Dans ce cas, $B = AD = 0$ et en prenant par exemple $\lambda = 1 \in \mathbb{K}^\star$, on a : $A = \lambda B$.

∗ Deuxième cas : $A \neq 0$.
Dans ce cas, $A(1 - DC) = 0$ implique que $DC = 1$, c'est-à-dire que D est un élément inversible de $\mathbb{K}[X]$. D'après la proposition 7.2.3.2, $D = \lambda \in \mathbb{K}^\star$. Par suite, $B = AD = DA = \lambda A$ avec $\lambda \in \mathbb{K}^\star$.

⊠

Ceci nous amène à poser la définition suivante.

Définition 7.3.1.6 On dit que deux polynômes A et B sont associés s'il existe $\lambda \in \mathbb{K}^\star$ tel que $B = \lambda A$.

Remarques :

- *ainsi $A|B$ et $B|A$ si et seulement si A et B sont associés ;*
- *la relation « est associé à » est une relation d'équivalence sur $\mathbb{K}[X]$;*
- *dans $\mathbb{Z}$, on a finalement deux critères pour déterminer si un entier donné divise un autre : soit on effectue la division euclidienne et on montre que le reste est nul, soit on connaît la factorisation de l'entier et on compare les facteurs premiers ainsi que les exposants dans cette décomposition. On va voir qu'on a en fait des raisonnements tout à fait semblables dans $\mathbb{K}[X]$, mais pour cela il faut commencer*

par définir la division euclidienne de deux polynômes et ce qu'est un polynôme « premier ». On parlera d'ailleurs plutôt de polynôme « irréductible » plutôt que de polynôme « premier ».

Définition 7.3.1.7 On dit qu'un polynôme $P \in \mathbb{K}[X]$ est irréductible dans $\mathbb{K}[X]$ si :

(i) $\deg(P) \geqslant 1$;

(ii) et les seuls diviseurs de P sont les polynômes associés à P et les éléments inversibles de $\mathbb{K}[X]$.

Remarque : *autrement dit, P est irréductible si $\deg(P) \geqslant 1$ et les seuls diviseurs de P sont les λP ou bien λ, avec $\lambda \in \mathbb{K}^\star$. On peut aussi reformuler en langage mathématique : un polynôme non constant (c'est-à-dire de degré supérieur ou égal à 1) est irréductible si*

$$\forall Q \in \mathbb{K}[X] \ , \ (Q|P \Longrightarrow (Q \in \mathbb{K}^\star \ \textit{ou} \ \exists \lambda \in \mathbb{K}^\star \ , \ Q = \lambda P))$$

On peut aussi reformuler cela de façon équivalente :

$$\forall Q \in \mathbb{K}[X] \ , \ (Q|P \Longrightarrow (\deg(Q) = 0 \quad \textit{ou} \quad \deg(Q) = \deg(P)))$$

Proposition 7.3.1.8 *Tout polynôme de degré 1 est irréductible.*

Preuve :

Soit $P \in \mathbb{K}[X]$ tel que $\deg(P) = 1$. Montrons que P est irréductible.
Soit Q un diviseur de P dans $\mathbb{K}[X]$. Il existe $A \in \mathbb{K}[X]$ tel que $P = QA$. En prenant les degrés, il vient $1 = \deg(P) = \deg(A) + \deg(Q)$. Or, $\deg(A)$ et $\deg(Q)$ appartiennent à $\mathbb{N} \cup \{-\infty\}$ donc il y a deux cas :

- soit $\deg(A) = 1$ et $\deg(Q) = 0$ et dans ce cas, $Q \in \mathbb{K}^\star$;
- ou bien $\deg(Q) = 1$ et $\deg(A) = 0$, et dans ce cas cas, $A = \lambda \in \mathbb{K}^\star$ et $P = QA = \lambda Q$.

Ce qui prouve que les seuls diviseurs de P sont bien les éléments inversibles de $\mathbb{K}[X]$ et les polynômes associés à P, c'est-à-dire P est irréductible.

⊠

⚠ **Attention :** un polynôme constant n'est pas irréductible par définition !

Exemple 7.3.1.9 X^2-1 n'est pas irréductible dans $\mathbb{R}[X]$ car $(X-1)|(X^2-1)$ et $X-1$ n'est ni inversible, ni associé à X^2-1.

Exemple 7.3.1.10 X^2+X+1 est irréductible dans $\mathbb{R}[X]$ mais ne l'est pas dans $\mathbb{C}[X]$. En effet, dans $\mathbb{C}[X]$, on a :

$$X^2+X+1=(X-j)(X-\overline{j}) \quad \text{avec } j=e^{i\frac{2\pi}{3}}$$

Par ailleurs, si $X^2+X+1=AB$ avec $A,B\in\mathbb{R}[X]$ et $\deg(A)>0$ et $\deg(B)>0$, alors $\deg(A)=\deg(B)=1$. Il existe alors $a,b,c,d\in\mathbb{R}$ tels que :

$$X^2+X+1=(aX+b)(cX+d)$$

En développant et en identifiant les coefficients, on obtient : $ac=bd=1$ et $ad+bc=1$. Il s'ensuit que $a\neq 0$, $b\neq 0$ et $\frac{a}{b}+\frac{b}{a}=1$. Alors $1=\frac{a}{b}+\frac{b}{a}\geqslant 2\sqrt{\frac{a}{b}\times\frac{b}{a}}=2$, ce qui est absurde. Ce qui prouve que si $X^2+X+1=AB$, alors $\deg(A)=0$ ou $\deg(B)=0$. Par suite, X^2+X+1 est bien irréductible dans $\mathbb{R}[X]$.

Exemple 7.3.1.11 X^8+1 n'est pas irréductible dans $\mathbb{R}[X]$ car :

$$X^8+1=(X^2-\sqrt{2+\sqrt{2}}X+1)(X^2+\sqrt{2+\sqrt{2}}X+1)(X^2-\sqrt{2-\sqrt{2}}X+1)(X^2+\sqrt{2-\sqrt{2}}X+1)$$

Remarque : *dans ces deux exemples, pour montrer que X^2+X+1 est irréductible dans $\mathbb{R}[X]$ à partir de la définition, c'est assez « pénible ». De même, trouver la factorisation de X^8+1 n'est pas « évident ». On verra un peu plus loin une méthode beaucoup plus simple qui utilise les racines d'un polynôme : avec cette méthode, les deux exemples sont faciles à traiter.*

⚠ **Attention :** dans cet exemple, on a vu que X^2+X+1 est irréductible dans $\mathbb{R}[X]$ mais pas dans $\mathbb{C}[X]$. Il faudra donc faire bien attention à préciser (si le contexte n'est pas clair) irréductible dans quoi !

7.3.2 Division euclidienne dans $\mathbb{K}[X]$

Théorème 7.3.2.1 (Division euclidienne) *Soient A et B deux polynômes. On suppose que $A\neq 0$. Alors il existe un unique couple $(Q,R)\in\mathbb{K}[X]^2$ tel que :*

$$B=QA+R \qquad et \qquad \deg R<\deg A$$

L'écriture $B=QA+R$ est appelée la division euclidienne de B par A, Q est le quotient de la division euclidienne de B par A, et R le reste.

Preuve :

• Pour commencer, si $A = \lambda \in \mathbb{K}^\star$ est un polynôme constant (non nul), c'est clair car alors le reste doit être nul et on obtient donc $Q = \lambda^{-1}B$. Ce qui montre l'existence et l'unicité.

• On suppose donc $p = \deg(A) \geqslant 1$.

∗ Montrons l'unicité (sous réserve d'existence).

On suppose qu'il existe deux couples (Q_1, R_1) et (Q_2, R_2) vérifiant les conditions de l'énoncé, c'est-à-dire :

$$B = Q_1A + R_1 \ \ ; \ \ B = Q_2A + R_2$$

avec

$$\deg(R_1) < \deg(A) \ \text{ et } \ \deg(R_2) < \deg(A)$$

On a alors : $R_2 - R_1 = A(Q_1 - Q_2)$. En prenant les degrés, il vient $\deg(R_2 - R_1) = \deg A + \deg(Q_1 - Q_2)$ et donc :

$$\deg(Q_1 - Q_2) = \deg(R_2 - R_1) - \deg A$$

Or, $\mathbb{K}_{p-1}[X]$ est un sous-espace vectoriel de $\mathbb{K}[X]$ et par hypothèse $R_1, R_2 \in \mathbb{K}_{p-1}[X]$, donc $R_2 - R_1 \in \mathbb{K}_{p-1}[X]$ et par suite,

$$\deg(Q_1 - Q_2) = \deg(R_2 - R_1) - \deg A \leqslant p - 1 - p < 0$$

Ceci impose que $Q_1 - Q_2 = 0$, c'est-à-dire $Q_1 = Q_2$. D'où, en remplaçant, $R_2 = R_1$ et l'unicité est prouvée.

∗ Montrons à présent l'existence.

Si $B = 0$, le couple $(Q, R) = (0, 0)$ convient. On suppose à présent que $B \neq 0$. Montrons alors l'existence par récurrence forte sur $n = \deg(B) \in \mathbb{N}$.

Initialisation :

Si B est de degré 0, c'est-à-dire constant, on a compte-tenu de l'hypothèse $\deg(A) = p \geqslant 1$, $B = 0 \times A + B$. En posant $Q = 0$ et $R = B$, on a donc $B = QA + R$ avec $\deg(R) < \deg(A)$. Ce qui prouve que la propriété est vraie au rang $n = 0$.

Hérédité :

On suppose que pour un entier n, la propriété est vraie jusqu'au rang n. Montrons qu'elle est vraie au rang $n + 1$. Soit B un polynôme de degré $n + 1$.

On distingue deux cas :

- ▷ si $n+1 < p$, alors à nouveau le couple $(0, B)$ convient ;
- ▷ Sinon, soit b_{n+1} le coefficient dominant de B et a_p le coefficient dominant de A. On a donc $a_p \neq 0$ et $b_{n+1} \neq 0$. Alors :

$$B_1 = B - \frac{b_{n+1}}{a_p} X^{n+1-p} A$$

est un polynôme de degré au plus n. On applique l'hypothèse de récurrence : il existe Q_1 et R deux polynômes tels que $B_1 = Q_1 A + R$ avec $\deg R < p$. Alors :

$$B = B_1 + \frac{b_{n+1}}{a_p} X^{n+1-p} A = \left(\frac{b_{n+1}}{a_p} X^{n+1-p} + Q_1 \right) A + R$$

Ce qui prouve l'existence et montre que la propriété est vraie au rang $n+1$. Ceci achève la récurrence et termine la preuve du théorème.

⊠

Remarque : *la méthode pratique pour déterminer le quotient et le reste est justement celle décrite par la démonstration.*

Exemple 7.3.2.2 Soient $A = X^3 + X - 1$ et $B = X^5 + X^4 + X^3 + X^2 + X + 1$. On veut effectuer la division euclidienne de B par A.

- On commence, comme dans la preuve, par écrire :

$$B = X^2 A + X^4 + 2X^2 + X + 1$$

- puis on recommence avec $B_1 = X^4 + 2X^2 + X + 1$:

$$B_1 = XA + X^2 + 2X + 1$$

- ici, on obtient $B_2 = X^2 + 2X + 1$ et $\deg(B_2) < \deg(A)$ donc B_2 est le reste de la division euclidienne et on s'arrête.

Ainsi, $B = (X^2 + X)A + X^2 + 2X + 1$ est la division euclidienne de B par A. Dans la pratique, on présente les calculs plutôt sous la forme suivante :

$$\begin{array}{l|l} X^5 + X^4 + X^3 + X^2 + X + 1 & X^3 + X - 1 \\ \hline -X^2(X^3 + X - 1) & X^2 + X \\ \hline \quad X^4 + 2X^2 + X + 1 & \\ \quad -X(X^3 + X - 1) & \\ \hline \qquad X^2 + 2X + 1 & \end{array}$$

Exercice 7.3.2.3 Effectuer la division euclidienne de $X^5 + 5X^4 - 3X^3 + 2X^2 + X + 1$ par $X^2 + X + 1$.

Exercice 7.3.2.4 Déterminer le quotient et le reste de la division euclidienne du polynôme $X^6 - X^4 + X^3 - X^2 + X - 1$ par $X^2 + 1$.

La division euclidienne est aussi pratique pour le calcul de primitives de fonctions rationnelles.

Exercice 7.3.2.5 Soient $B = X^4 + 3X^2 + 3X - 1$ et $A = X^2 + 1$.

1. Déterminer le quotient et le reste de la division euclidienne de B par A.
2. En déduire une primitive sur $\mathbb{R}$ de la fonction $f : x \longmapsto \dfrac{x^4 + 3x^2 + 3x - 1}{x^2 + 1}$.

Proposition 7.3.2.6 *La division euclidienne est linéaire dans le sens où si $A \in \mathbb{K}[X]$ et $A \neq 0$, alors :*

$$\forall (B, C) \in \mathbb{K}[X]^2 \ , \ \forall (\lambda, \mu) \in \mathbb{K}^2 \ , \ quot_A(\lambda B + \mu C) = \lambda \, quot_A(B) + \mu \, quot_A(C)$$

et

$$\forall (B, C) \in \mathbb{K}[X]^2 \ , \ \forall (\lambda, \mu) \in \mathbb{K}^2 \ , \ rest_A(\lambda B + \mu C) = \lambda \, rest_A(B) + \mu \, rest_A(C)$$

où $quot_A$ désigne le quotient de la division euclidienne par A et $rest_A$ le reste.

Preuve :

Soient $(B, C) \in \mathbb{K}[X]^2$ et $(\lambda, \mu) \in \mathbb{K}^2$. Par définition du quotient et du reste de la division euclidienne, on a :

$$B = A \times \mathrm{quot}_A(B) + \mathrm{rest}_A(B) \ \text{ et } \ C = A \times \mathrm{quot}_A(C) + \mathrm{rest}_A(C)$$

avec $\deg(\mathrm{rest}_A(B)) < \deg(A)$ et $\deg(\mathrm{rest}_A(C)) < \deg(A)$. Il s'ensuit que :

$$\lambda B + \mu C = (\lambda \, \mathrm{quot}_A(B) + \mu \, \mathrm{quot}_A(C)) \, A + (\lambda \, \mathrm{rest}_A(B) + \mu \, \mathrm{rest}_A(C))$$

avec $\deg(\lambda \, \mathrm{rest}_A(B) + \mu \, \mathrm{rest}_A(C)) < \deg(A)$. Par unicité du quotient et du reste de la division euclidienne,

$$\mathrm{quot}_A(\lambda B + \mu C) = \lambda \, \mathrm{quot}_A(B) + \mu \, \mathrm{quot}_A(C)$$

et

$$\mathrm{rest}_A(\lambda B + \mu C) = \lambda \, \mathrm{rest}_A(B) + \mu \, \mathrm{rest}_A(C)$$

⊠

Proposition 7.3.2.7 *Soient $A, B \in \mathbb{K}[X]$ avec $A \neq 0$. $A|B$ si et seulement si le reste de la division euclidienne de B par A est nul.*

Exercice 7.3.2.8 Soit $A \in \mathbb{K}[X] \setminus \{0\}$ et soit rest_A l'application de $\mathbb{K}[X]$ dans lui-même, qui à un polynôme P associe le reste de la division euclidienne de P par A.

1. Montrer que rest_A est un projecteur de $\mathbb{K}[X]$.
2. Déterminer le noyau et l'image de rest_A.
3. En déduire que $A\mathbb{K}[X]$ est un sous-espace vectoriel de $\mathbb{K}[X]$ et que si $n = \deg(A)$ (avec $n \geqslant 1$) alors :
$$A\mathbb{K}[X] \oplus \mathbb{K}_{n-1}[X] = \mathbb{K}[X]$$

7.3.3 Idéaux de $\mathbb{K}[X]$

On a vu dans le cours d'arithmétique que les sous-groupes de $\mathbb{Z}$ sont les $n\mathbb{Z}$ avec $n \in \mathbb{N}$. En réalité, un sous-groupe de $\mathbb{Z}$ est aussi stable par multiplication par les éléments de $\mathbb{Z}$: c'est ce qui nous amène à poser la définition suivante.

Définition 7.3.3.1 Soit $\mathcal{I} \subset \mathbb{K}[X]$. On dit que $\mathcal{I}$ est un idéal de $\mathbb{K}[X]$ si :

(i) $(\mathcal{I}, +)$ est un sous-groupe de $\mathbb{K}[X]$;

(ii) $\forall A \in \mathcal{I}$, $\forall P \in \mathbb{K}[X]$, $P \times A \in \mathcal{I}$.

Proposition 7.3.3.2 *Soit $\mathcal{I} \subset \mathbb{K}[X]$. Alors $\mathcal{I}$ est un idéal de $\mathbb{K}[X]$ si et seulement si :*

(i) $0 \in \mathcal{I}$;
(ii) $\forall A, B \in \mathcal{I}$, $\forall P, Q \in \mathbb{K}[X]$, $PA + QB \in \mathcal{I}$.

Exercice 7.3.3.3 Prouver la proposition précédente.

Exemple 7.3.3.4 Si $A \in \mathbb{K}[X]$, alors $A\mathbb{K}[X]$ est un idéal de $\mathbb{K}[X]$. En effet,

(i) $A|0$ donc $0 \in A\mathbb{K}[X]$;

(ii) Si $B, C \in A\mathbb{K}[X]$ et $P, Q \in \mathbb{K}[X]$, alors $A|B$ et $A|C$ donc, $A|(PB + QC)$, c'est-à-dire $PB + QC \in A\mathbb{K}[X]$.

Théorème 7.3.3.5 *Soit $\mathcal{I} \subset \mathbb{K}[X]$. Alors les énoncés suivants sont équivalents :*

(i) $\mathcal{I}$ est un idéal de $\mathbb{K}[X]$;

(ii) il existe $A \in \mathbb{K}[X]$ tel que $\mathcal{I} = A\mathbb{K}[X]$.

Preuve :

• $(ii) \Longrightarrow (i)$
C'est ce qu'on vient de voir en exemple.

• $(i) \Longrightarrow (ii)$

Soit $\mathcal{I}$ un idéal de $\mathbb{K}[X]$. Si $\mathcal{I} = \{0\}$, alors $\mathcal{I} = 0\mathbb{K}[X]$ et le résultat est prouvé. On suppose donc $\mathcal{I} \neq \{0\}$.

Considérons l'ensemble $J = \{\deg(P)\ ,\ P \in \mathcal{I} \setminus \{0\}\}$. Alors, J est une partie non vide de $\mathbb{N}$ (puisque par hypothèse, $\mathcal{I}\setminus\{0\} \neq \emptyset$). Par conséquent, elle admet un plus petit élément. Soit $A \in \mathcal{I}\setminus\{0\}$ tel que $\deg(A) = \min J$. Montrons que $\mathcal{I} = A\mathbb{K}[X]$.

∗ Montrons que $A\mathbb{K}[X] \subset \mathcal{I}$.

Puisque $A \in \mathcal{I}$ et que $\mathcal{I}$ est un idéal de $\mathbb{K}[X]$, on a :

$$\forall P \in \mathbb{K}[X]\ ,\ AP \in \mathcal{I}$$

Par suite, $A\mathbb{K}[X] \subset \mathcal{I}$.

∗ Montrons que $\mathcal{I} \subset A\mathbb{K}[X]$.

Soit $B \in \mathcal{I}$. Puisque $A \neq 0$, on peut faire la division euclidienne de B par A : il existe (un unique) $(Q, R) \in \mathbb{K}[X]^2$ tel que :

$$B = QA + R \quad \text{et} \quad \deg(R) < \deg(A)$$

Par ailleurs, $A \in \mathcal{I}$ donc $QA \in \mathcal{I}$ ($\mathcal{I}$ est un idéal). De plus, $B \in \mathcal{I}$. Par conséquent, $B - QA \in \mathcal{I}$, c'est-à-dire $R \in \mathcal{I}$. Ainsi, $R \in \mathcal{I}$ et $\deg(R) < \deg(A)$ avec $\deg(A) = \min\{\deg(P)\ ,\ P \in \mathcal{I} \setminus \{0\}\}$. D'où l'on déduit que $R = 0$, c'est-à-dire $B = QA \in A\mathbb{K}[X]$.

⊠

Remarques :

- *on a déjà vu que $A\mathbb{K}[X] = B\mathbb{K}[X]$ si et seulement si A et B sont associés ;*
- *lorsque $\mathcal{I} \neq \{0\}$, il existe un unique polynôme unitaire A tel que $\mathcal{I} = A\mathbb{K}[X]$.*

7.3.4 Polynômes premiers entre eux

Théorème 7.3.4.1 (Définition) *Soient A et B deux polynômes non nuls.*

- *Il existe un unique polynôme unitaire, appelé plus grand commun diviseur de A et B et noté $A \wedge B$ ou $pgcd(A, B)$, tel que :*

$$A\mathbb{K}[X] + B\mathbb{K}[X] = pgcd(A, B)\mathbb{K}[X]$$

Cet unique polynôme unitaire est le polynôme unitaire de degré maximal qui divise A et B.

- *Il existe un unique polynôme unitaire, appelé plus petit commun multiple de A et B et noté $A \vee B$ ou $ppcm(A, B)$, tel que :*

$$A\mathbb{K}[X] \cap B\mathbb{K}[X] = ppcm(A, B)\mathbb{K}[X]$$

Cet unique polynôme unitaire est le polynôme unitaire de degré minimal parmi les multiples communs non nuls de A et de B.

Preuve :

• Soit $\mathcal{I} = A\mathbb{K}[X] + B\mathbb{K}[X] = \{PA + QB \ , \ (P, Q) \in \mathbb{K}[X]^2\}$.
On vérifie (le faire) que $\mathcal{I}$ est un idéal de $\mathbb{K}[X]$ et que $\mathcal{I} \neq \{0\}$. Par conséquent, d'après le théorème précédent, il existe un unique polynôme unitaire $\text{pgcd}(A, B)$ tel que :

$$A\mathbb{K}[X] + B\mathbb{K}[X] = \text{pgcd}(A, B)\mathbb{K}[X]$$

∗ Ensuite, $A \in A\mathbb{K}[X] \subset A\mathbb{K}[X] + B\mathbb{K}[X] = \text{pgcd}(A, B)\mathbb{K}[X]$. Par conséquent, $\text{pgcd}(A, B)|A$. De même, $\text{pgcd}(A, B)|B$. Par suite, $\text{pgcd}(A, B)$ est bien un polynôme unitaire qui divise A et B.

∗ Par ailleurs, si P est un diviseur commun de A et B, alors il existe $D, C \in \mathbb{K}[X]$ tels que $A = PC$ et $B = PD$. De plus, $\text{pgcd}(A, B) \in A\mathbb{K}[X] + B\mathbb{K}[X]$ donc il existe $(U, V) \in \mathbb{K}[X]^2$ tel que : $\text{pgcd}(A, B) = UA + VB$. On en déduit alors que :

$$\text{pgcd}(A, B) = UA + VB = (UC + VD)P$$

Puisque $\text{pgcd}(A, B) \neq 0$, $UC + VD \neq 0$ et donc :

$$\deg(\text{pgcd}(A, B)) = \deg(UC + VD) + \deg(P) \geqslant \deg(P)$$

Ce qui montre que $\text{pgcd}(A, B)$ est bien un diviseur commun de A et B, unitaire et de degré maximal parmi les diviseurs communs de A et B.

∗ Enfin, si P est unitaire et de degré maximal parmi les diviseurs communs de A et B, alors $\deg(P) \geqslant \deg(\text{pgcd}(A,B))$ et d'après le point qui précède, $\deg(P) \leqslant \deg(\text{pgcd}(A,B))$. Par suite, $\deg(P) = \deg(\text{pgcd}(A,B))$ et donc $\deg(UC+VD) = 0$, c'est-à-dire $UC + VD \in \mathbb{K}^\star$. Ce qui prouve que P et $\text{pgcd}(A,B)$ sont associés. Étant tous deux unitaires, ils sont donc égaux.

• De la même façon, on montre que $A\mathbb{K}[X] \cap B\mathbb{K}[X]$ est un idéal de $\mathbb{K}[X]$, non réduit à $\{0\}$ (il contient AB qui est non nul). Il existe donc un unique polynôme unitaire $\text{ppcm}(A,B)$ tel que :

$$A\mathbb{K}[X] \cap B\mathbb{K}[X] = \text{ppcm}(A,B)\mathbb{K}[X]$$

Ensuite,

∗ d'une part, $\text{ppcm}(A,B) \in \text{ppcm}(A,B)\mathbb{K}[X] = (A\mathbb{K}[X] \cap B\mathbb{K}[X])$. Par suite, $\text{ppcm}(A,B) \in A\mathbb{K}[X]$, c'est-à-dire $A|\text{ppcm}(A,B)$. De même, $B|\text{ppcm}(A,B)$. Ce qui montre que $\text{ppcm}(A,B)$ est un polynôme unitaire qui est un multiple de A et B ;

∗ d'autre part, si $P \neq 0$ est un multiple de A et de B, alors $A|P$ et $B|P$, c'est-à-dire $P \in A\mathbb{K}[X] \cap B\mathbb{K}[X] = \text{ppcm}(A,B)\mathbb{K}[X]$. Il s'ensuit que $\text{ppcm}(A,B)|P$ et puisque $P \neq 0$,

$$\deg(\text{ppcm}(A,B)) \leqslant \deg(P)$$

Ceci prouve que $\text{ppcm}(A,B)$ est de degré minimal parmi les multiples communs non nuls de A et B ;

∗ enfin, si on suppose que P est unitaire (et donc non nul) et de degré minimal parmi les multiples communs de A et B, alors $\deg(P) \leqslant \deg(\text{ppcm}(A,B))$ et par suite, on a égalité. On conclut alors, comme dans le premier cas, que P et $\text{ppcm}(A,B)$ sont égaux (car associés et unitaires).

⊠

Remarque : *en fait la démonstration montre que, comme pour $\mathbb{Z}$, on a :*

$$\begin{cases} P|A \\ P|B \end{cases} \iff P|pgcd(A,B) \quad et \quad \begin{cases} A|P \\ B|P \end{cases} \iff ppcm(A,B)|P$$

Définition 7.3.4.2 Soient A et B deux polynômes dans $\mathbb{K}[X]$ et non nuls. On dit que A et B sont premiers entre eux si $\text{pgcd}(A,B) = 1$.

Remarque : *autrement dit, A et B sont premiers entre eux si les seuls diviseurs communs de A et B sont les polynômes constants (non nuls).*

Exemple 7.3.4.3 Si $A = X - 1$ et $B = X$, alors A et B sont premiers entre eux.

Algorithme d'Euclide : tout comme dans $\mathbb{Z}$, on peut utiliser l'algorithme d'Euclide pour déterminer le pgcd de deux polynômes.

Exemple 7.3.4.4 Soient $A = X^4 + X^2 + 1$ et $B = X^5 - 2X^4 + 4X^3 - 2X^2 + X + 1$. Déterminons le pgcd de A et B.

$$\begin{aligned} B &= (X-2) \times A + 3X^3 + 3 \\ A &= \frac{1}{3}X(3X^3+3) + X^2 - X + 1 \\ 3X^3 + 3 &= (3X+3)(X^2 - X + 1) \end{aligned}$$

Le dernier reste non nul est $X^2 - X + 1$. On en déduit alors que $\text{pgcd}(A, B) = X^2 - X + 1$.

Remarque : *dans $\mathbb{Z}$, on a vu une autre méthode pour déterminer le pgcd de deux entiers, qui utilise la décomposition en facteurs premiers. On reverra plus loin qu'on dispose aussi de cette méthode dans $\mathbb{K}[X]$.*

7.3.5 Théorème de Bézout et théorème de Gauss

Théorème 7.3.5.1 (théorème de Bézout) *Soient A et B deux éléments non nuls de $\mathbb{K}[X]$. Alors :*

$$A \wedge B = 1 \iff \exists (U, V) \in \mathbb{K}[X]^2 \ , \ UA + VB = 1$$

Preuve :

La démonstration est identique à la démonstration dans $\mathbb{Z}$.

• On suppose que $A \wedge B = 1$.
Alors $A\mathbb{K}[X] + B\mathbb{K}[X] = (A \wedge B)\mathbb{K}[X] = \mathbb{K}[X]$. En particulier, puisque $1 \in \mathbb{K}[X]$, il existe $U \in \mathbb{K}[X]$ et $V \in \mathbb{K}[X]$ tels que $UA + VB = 1$.

• Réciproquement, s'il existe $(U, V) \in \mathbb{K}[X]^2$ tel que $UA + VB = 1$, alors $1 \in A\mathbb{K}[X] + B\mathbb{K}[X]$. Or, on a déjà vu que $A\mathbb{K}[X] + B\mathbb{K}[X]$ est un idéal de $\mathbb{K}[X]$. Par suite : $\forall P \in \mathbb{K}[X]$, $P = P \times 1 \in A\mathbb{K}[X] + B\mathbb{K}[X]$.
Ce qui prouve que $\text{pgcd}(A, B)\mathbb{K}[X] = A\mathbb{K}[X] + B\mathbb{K}[X] = \mathbb{K}[X]$. Il s'ensuit que 1 et $\text{pgcd}(A, B)$ sont associés et tout deux unitaires donc $\text{pgcd}(A, B) = 1$.

⊠

Théorème 7.3.5.2 (théorème de Gauss) *Soient A, B, C trois polynômes non nuls. Alors :*

$$\begin{cases} A|BC \\ A \wedge B = 1 \end{cases} \implies A|C$$

Preuve :

À nouveau, la preuve est identique à la démonstration dans $\mathbb{Z}$.
On suppose que $A \wedge B = 1$ et que $A|BC$. D'après le théorème de Bézout, il existe deux polynômes U et V tels que :

$$UA + VB = 1$$

Alors $C = UCA + VBC$. Or, $A|UCA$ et $A|VBC$ donc $A|C$.

⊠

Théorème 7.3.5.3 (relation de Bézout améliorée) *Soient $A, B \in \mathbb{K}[X]$ tels que $\deg(A) \geqslant 1$, $\deg(B) \geqslant 1$ et $A \wedge B = 1$. Alors il existe un unique couple $(U, V) \in \mathbb{K}[X]^2$ tel que :*

$$UA + VB = 1 \quad \text{et} \quad \deg(U) < \deg(B) \quad \text{et} \quad \deg(V) < \deg(A)$$

Preuve :

• Montrons l'existence.
D'après le théorème de Bézout, on sait qu'il existe $(U, V) \in \mathbb{K}[X]^2$ tel que : $UA + VB = 1$. On fait alors la division euclidienne de U par B : il existe $(Q_1, R_1) \in \mathbb{K}[X]^2$ tel que $U = Q_1 B + R_1$ et $\deg(R_1) < \deg(B)$. On a alors :

$$R_1 A + (V + Q_1 A)B = 1$$

Si $R_1 = 0$, alors $B(V + Q_1 A) = 1$ et donc B est inversible, ce qui est absurde car $\deg(B) \geqslant 1$. On en déduit que $0 \leqslant \deg(R_1)$. En notant $R_2 = V + Q_1 A$, on a $R_2 B = 1 - R_1 A$. En prenant les degrés on obtient :

$$\deg(R_2) + \deg(B) = \deg(1 - R_1 A) = \deg(R_1 A) = \deg(R_1) + \deg(A)$$

(la seconde égalité découle du fait que $\deg(R_1 A) \geqslant 1 > \deg(1)$). Par conséquent,

$$\deg(R_2) = \deg(R_1) - \deg(B) + \deg(A) < \deg(A)$$

(puisque $\deg(R_1) < \deg(B)$). Ainsi le couple (R_1, R_2) convient.

• Montrons l'unicité.
Soient (U_1, V_1) et (U_2, V_2) deux couples vérifiant les conclusions du théorème. Alors :

$$(U_1 - U_2)A = (V_2 - V_1)B$$

Par suite, $A|(V_2 - V_1)B$ et $A \wedge B = 1$. D'après le théorème de Gauss, $A|(V_2 - V_1)$. Or, $\deg(V_2 - V_1) < \deg(A)$ donc $V_2 - V_1 = 0$, c'est-à-dire $V_1 = V_2$. En remplaçant dans la première égalité, on obtient $U_1 - U_2 = 0$ (car $\mathbb{K}[X]$ est intègre et $A \neq 0$), c'est-à-dire $U_1 = U_2$. Ce qui prouve l'unicité.

⊠

7.4 Racines d'un polynôme

7.4.1 Fonction polynomiale associée à un polynôme

Définition 7.4.1.1 Soit $P \in \mathbb{K}[X]$, avec $P = \sum_{k=0}^{n} a_k X^k$ ($n \in \mathbb{N}$ et $(a_k)_{0 \leqslant k \leqslant n} \in \mathbb{K}^{n+1}$). Pour $x \in \mathbb{K}$, on pose : $\widetilde{P}(x) = \sum_{k=0}^{n} a_k x^k$. L'application $x \longmapsto \widetilde{P}(x)$ est appelée fonction polynomiale associée à P.

Remarques :

- *la différence fondamentale entre polynôme et fonction polynomiale est que pour un polynôme, l'indéterminée X est fixée : c'est un « symbole » qui désigne la suite $(\delta_1(n))_{n\in\mathbb{N}}$ et il n'y a aucun sens à dire « on évalue en $X = 1$ ou $X = 3$ », alors que pour une fonction polynomiale, le « x » est une variable qui varie dans l'ensemble de définition de $\widetilde{P}$;*
- *plus précisément, on peut choisir comme ensemble de définition pour $\widetilde{P}$ toute partie I de $\mathbb{K}$. On obtient alors une application $\widetilde{P} \in \mathcal{F}(I, \mathbb{K})$. En toute rigueur, il faudrait donc préciser l'ensemble de définition et noter $\widetilde{P}_I$, ce qu'on ne fait pas dans la pratique ;*
- *si $f \in \mathcal{F}(I, \mathbb{K})$, par définition f est polynomiale s'il existe $P \in \mathbb{K}[X]$ tel que $f = \tilde{P}$;*
- *d'un point de vue mathématique, P et $\tilde{P}$ sont deux objets différents. Ceci étant dit, on a envie de dire que « c'est la même chose » : il suffit de remplacer « X » par « x ». Dans ce qui suit, on va traduire rigoureusement cette identification et voire sous quelles conditions on peut identifier P et $\tilde{P}$.*

Proposition 7.4.1.2 *Soit $I \subset \mathbb{K}$ (I non vide) et soit $\varphi : \mathbb{K}[X] \longrightarrow \mathcal{F}(I, \mathbb{K})$ définie par $\varphi(P) = \widetilde{P}$ pour tout $P \in \mathbb{K}[X]$. Alors :*

(i) $\forall (P,Q) \in \mathbb{K}[X]^2$, $\forall x \in I$, $\widetilde{P+Q}(x) = \widetilde{P}(x) + \widetilde{Q}(x)$.

(ii) $\forall \lambda \in \mathbb{K}$, $\forall P \in \mathbb{K}[X]$, $\forall x \in I$, $\widetilde{\lambda \cdot P}(x) = \lambda \times \widetilde{P}(x)$.

(iii) $\forall (P,Q) \in \mathbb{K}[X]^2$, $\forall x \in I$, $\widetilde{P \times Q}(x) = \widetilde{P}(x) \times \widetilde{Q}(x)$.

(iv) $\forall x \in I$, $\widetilde{1}(x) = 1$.

(v) Plus généralement, si $P = c \in \mathbb{K}$ est un polynôme constant, alors : $\forall x \in I$, $\widetilde{c}(x) = c$.

Autrement dit, l'application φ est un morphisme d'algèbres.

Preuve :

C'est clair ! Ceci découle de la construction même des polynômes. ⊠

Objectif : on veut pouvoir identifier l'ensemble $\mathbb{K}[X]$ avec $\mathrm{Im}\varphi$, c'est-à-dire identifier un polynôme et sa fonction polynomiale associée. Pour pouvoir faire cette identification, il faut que deux polynômes distincts donnent deux fonctions polynomiales distinctes, c'est-à-dire que φ soit injective, ce qui n'est pas toujours le cas. Par exemple, si $I = \{0, 1\}$ et $P = X$ et $Q = 2X^2 - X$, on a $\widetilde{P}_I = \widetilde{Q}_I$. On va montrer juste après que si I est infini, on peut faire cette identification et du coup, on notera de façon identique P et $\widetilde{P}$.

7.4.2 Racines d'un polynôme

Définition 7.4.2.1 Soient $P \in \mathbb{K}[X]$ et $a \in \mathbb{K}$. On dit que a est une racine de P si $\widetilde{P}(a) = 0$.

Exemple 7.4.2.2 Soit $P = X^2 + X + 1$. Alors j est une racine de P puisque $\widetilde{P}(j) = 1 + j + j^2 = 0$.

Proposition 7.4.2.3 *Soient $P \in \mathbb{K}[X]$ et $a \in \mathbb{K}$, alors le reste de la division euclidienne de P par $X - a$ est $R = \widetilde{P}(a)$.*

Preuve :

En effet, si $P = Q \times (X-a) + R$ avec $\deg(R) < \deg(X-a)$, alors $R \in \mathbb{K}$. On a alors :

$$\widetilde{P}(a) = \widetilde{((X-a)Q + R)}(a) = \widetilde{Q}(a) \times 0 + \widetilde{R}(a) = \widetilde{R}(a) = R$$

⊠

Corollaire 7.4.2.4 *Soient $P \in \mathbb{K}[X]$ et $a \in \mathbb{K}$. Alors a est une racine de P si et seulement si $X - a$ divise P.*

Preuve :

On vient de voir que le reste de la division euclidienne de P par $X - a$ est $R = \widetilde{P}(a)$. Par suite,

$$(X-a)|P \iff R = 0 \iff \widetilde{P}(a) = 0$$

⊠

Exercice 7.4.2.5 Proposer une démonstration directe de ce résultat en utilisant la formule de Bernoulli (voir proposition 1.2.3.9).

Proposition 7.4.2.6 *Soient $P \in \mathbb{K}[X]$, $n \in \mathbb{N}^\star$. On suppose que $a_1, \cdots, a_n \in \mathbb{K}$ sont des racines de P, deux à deux distinctes. Alors $(X-a_1) \times \cdots \times (X-a_n)$ divise P. De plus, si $P \neq 0$, alors $n \leqslant \deg(P)$.*

Preuve :

On montre par récurrence finie sur $k \in [\![1, n]\!]$ que $\prod_{i=1}^{k}(X-a_i)|P$.

Initialisation :

Pour $k = 1$, c'est la proposition précédente.

Hérédité :

On suppose la propriété vraie au rang k avec $1 \leqslant k < n$. Alors, il existe $Q \in \mathbb{K}[X]$ tel que :

$$P = Q \times \prod_{i=1}^{k}(X-a_i)$$

On a alors :

$$0 = \widetilde{P}(a_{k+1}) = \widetilde{Q}(a_{k+1}) \times \prod_{i=1}^{k}(a_{k+1} - a_i) \text{ et } \prod_{i=1}^{k}(a_{k+1} - a_i) \neq 0$$

car les a_i (pour $1 \leqslant i \leqslant n$) sont deux à deux distincts. Par suite, $\widetilde{Q}(a_{k+1}) = 0$. D'après la proposition précédente, $(X - a_{k+1})|Q$ ce qui prouve que la propriété est vraie au rang $k+1$ et achève la récurrence.

⊠

Exercice 7.4.2.7 Quelle autre méthode « arithmétique » peut-on utiliser pour démontrer cette proposition ?

Corollaire 7.4.2.8 *Si P est un polynôme non nul, alors P a un nombre fini de racines distinctes. Plus précisément, P a au plus* $\deg(P)$ *racines distinctes.*

Proposition 7.4.2.9 *Si I est une partie infinie de $\mathbb{K}$, alors on peut identifier polynôme et fonction polynôme. Autrement dit, l'application $\varphi : \mathbb{K}[X] \longrightarrow \mathcal{F}(I, \mathbb{K})$, qui à un polynôme $P \in \mathbb{K}[X]$ associe $\tilde{P}$, est injective.*

Preuve :

Soit $P \in \ker \varphi$. Alors, $\widetilde{P} = 0$, c'est-à-dire $\forall x \in I$, $\widetilde{P}(x) = 0$. En particulier, P a donc une infinité de racines deux à deux distinctes, ce qui n'est possible que pour $P = 0$ d'après le corollaire précédent.

⊠

Conséquence : on n'écrit plus $\widetilde{P}$ et on notera $P(a)$ tout simplement au lieu de $\widetilde{P}(a)$.

7.4.3 Formule de Taylor et multiplicité d'une racine

Théorème 7.4.3.1 (Formule de Taylor) *Soient $P \in \mathbb{K}[X]$, $a \in \mathbb{K}$ et $n \geqslant \deg(P)$. Alors :*

$$P = \sum_{k=0}^{n} \frac{P^{(k)}(a)}{k!}(X - a)^k$$

Preuve :

Soit ψ l'application de $\mathbb{K}[X]$ dans $\mathbb{K}[X]$ définie par :

$$\forall P \in \mathbb{K}[X]\ ,\ \psi(P) = \sum_{k=0}^{+\infty} \frac{P^{(k)}(a)}{k!}(X-a)^k$$

• Tout d'abord, ψ est bien définie puisque si $P \in \mathbb{K}[X]$, alors pour tout entier $k > \deg(P)$, $P^{(k)} = 0$ et *a fortiori* $P^{(k)}(a) = 0$. Il s'ensuit que si $n \in \mathbb{N}$ et $n \geqslant \deg(P)$, alors :

$$\psi(P) = \sum_{k=0}^{+\infty} \frac{P^{(k)}(a)}{k!}(X-a)^k = \sum_{k=0}^{n} \frac{P^{(k)}(a)}{k!}(X-a)^k \in \mathbb{K}[X]$$

• Il est clair que ψ est un endomorphisme de $\mathbb{K}[X]$ car la dérivation est un endomorphisme de $\mathbb{K}[X]$, $P \mapsto \tilde{P}$ est linéaire, l'évaluation $e_a : f \mapsto f(a)$ est linéaire et la multiplication externe dans $\mathbb{K}[X]$ est linéaire.

• Ensuite, on détermine l'image par ψ du monôme X^p pour $p \in \mathbb{N}$. On a vu que :

$$D^k(X^p) = \begin{cases} \dfrac{p!}{(p-k)!}X^{p-k} & \text{si } k \leqslant p \\ 0 & \text{sinon} \end{cases}$$

Par suite, d'après la formule du binôme de Newton :

$$\psi(X^p) = \sum_{k=0}^{p} \frac{p!}{k!(p-k)!}a^{p-k}(X-a)^k = (X-a+a)^p = X^p$$

• Enfin, soit $P \in \mathbb{K}[X]$. Alors il existe $n \in \mathbb{N}$ et $(a_k)_{0\leqslant k\leqslant n} \in \mathbb{K}^{n+1}$ tels que :

$$P = \sum_{k=0}^{n} a_k X^k$$

Par linéarité,

$$\psi(P) = \sum_{k=0}^{n} a_k \psi(X^k) = \sum_{k=0}^{n} a_k X^k = P$$

⊠

Définition 7.4.3.2 Soient $P \in \mathbb{K}[X]$ et $a \in \mathbb{K}$. On dit que a est une racine d'ordre $m \in \mathbb{N}$ du polynôme P lorsque $(X-a)^m$ divise P et $(X-a)^{m+1}$ ne divise pas P.
On note alors $m = m_a(P)$ et $m_a(P)$ est appelé la multiplicité de la racine a pour P.

Remarques :

- *autrement dit, a est une racine d'ordre m pour P s'il existe $Q \in \mathbb{K}[X]$ tel que $P = (X-a)^m Q$ avec $Q(a) \neq 0$;*
- *par convention, pour le polynôme nul, on convient que $m_a(0) = +\infty$;*
- *on peut aussi reformuler en posant*

$$m_a(P) = \begin{cases} \max\{k \in \mathbb{N} \ / \ (X-a)^k | P\} & \text{si } P \neq 0 \\ +\infty & \text{si } P = 0 \end{cases}$$

Exemple 7.4.3.3 Si a n'est pas une racine de P, c'est une racine de multiplicité nulle.

Exemple 7.4.3.4 Soit $P = X(X-1)^2$. Alors,

- 1 est une racine de multiplicité deux : on dit aussi que c'est une racine double ;
- 0 est une racine de multiplicité un : on dit que c'est une racine simple de P.

Proposition 7.4.3.5 *Soient $P \in \mathbb{K}[X]$, $a \in \mathbb{K}$ et $m \in \mathbb{N}$. Alors :*

$$m_a(P) = m \iff \forall k \in [\![0, m-1]\!] \ , \ P^{(k)}(a) = 0 \quad et \quad P^{(m)}(a) \neq 0$$

Autrement dit, a est une racine de P de multiplicité m si les $m-1$ premières dérivées de P (en partant de la dérivée 0-ième) s'annulent en a, mais pas la m-ième.

Remarque : *de façon moins formelle,*

$$m = m_a(P) \iff 0 = P(a) = P'(a) = \cdots = P^{(m-1)}(a) = 0 \quad et \quad P^{(m)}(a) \neq 0$$

Preuve :

Le cas $m = 0$ est évident. On suppose donc $m \geqslant 1$.
D'après la formule de Taylor, si on fixe un entier $n \geqslant \deg(P)$, alors $n \geqslant m$ et :

$$\begin{aligned} P &= \sum_{k=0}^{n} \frac{P^{(k)}(a)}{k!}(X-a)^k \\ &= \sum_{k=0}^{m-1} \frac{P^{(k)}(a)}{k!}(X-a)^k + \sum_{k=m}^{n} \frac{P^{(k)}(a)}{k!}(X-a)^k \end{aligned}$$

On note alors :

$$P = \underbrace{\sum_{k=0}^{m-1} \frac{P^{(k)}(a)}{k!}(X-a)^k}_{R} + (X-a)^m \underbrace{\sum_{k=m}^{n} \frac{P^{(k)}(a)}{k!}(X-a)^{k-m}}_{Q}$$

Ainsi, on a $P = Q(X-a)^m + R$ avec $\deg R \leqslant m-1 < \deg(X-a)^m$. On en déduit que Q et R sont respectivement le quotient et le reste de la division euclidienne de P par $(X-a)^m$ (unicité du quotient et du reste). On a alors :

$$m = m_a(P) \iff R = 0 \quad \text{et} \quad Q(a) \neq 0$$

Or, d'une part, on a :

$$Q(a) = \frac{P^{(m)}(a)}{m!}$$

D'autre part, montrons que :

$$R = \sum_{k=0}^{m-1} r_k(X-a)^k = 0 \iff \forall k \in [\![0, m-1]\!] \ , \ r_k = 0$$

- $\Longleftarrow$ est évidente.
- Montrons $\Longrightarrow$.
  On suppose que $\sum_{k=0}^{m-1} r_k(X-a)^k = 0$. Alors la fonction polynomiale associée est nulle sur $\mathbb{K}$. On en déduit que :

  $$\forall x \in \mathbb{K} \ , \ R(x+a) = 0 \qquad \text{c'est-à-dire} \qquad \forall x \in \mathbb{K} \ , \ \sum_{k=0}^{m-1} r_k x^k = 0$$

  Puisque $\mathbb{K} = \mathbb{R}$ (ou $\mathbb{K} = \mathbb{C}$) est infini, d'après le paragraphe précédent, la fonction polynomiale est nulle si et seulement si le polynôme nul. Par suite, $\sum r_k X^k = 0$ (égalité entre polynômes), soit encore $r_k = 0$ pour tout entier k.

Ainsi,

$$\begin{aligned} m = m_a(P) &\iff R = 0 \quad \text{et} \quad Q(a) \neq 0 \\ &\iff \forall k \in [\![0, m-1]\!] \ , \ r_k = 0 \quad \text{et} \quad P^{(m)}(a) \neq 0 \\ &\iff \forall k \in [\![0, m-1]\!] \ , \ P^{(k)}(a) = 0 \quad \text{et} \quad P^{(m)}(a) \neq 0 \end{aligned}$$

⊠

Remarque : *cette caractérisation de la multiplicité d'une racine d'un polynôme est très utile dans la pratique. En effet, il est souvent plus facile de calculer les dérivées successives d'un polynôme puis d'évaluer en un point plutôt que de factoriser « à la main ».*

Proposition 7.4.3.6 *Pour tout $(P,Q) \in \mathbb{K}[X]^2$ et tout $a \in \mathbb{K}$, on a :*

$$m_a(PQ) = m_a(P) + m_a(Q) \qquad et \qquad m_a(P+Q) \geqslant \min\left(m_a(P), m_a(Q)\right)$$

Preuve :

Si $P = 0$ ou $Q = 0$, alors les propriétés sont évidentes. On suppose à présent $PQ \neq 0$, auquel cas $m_a(P)$ et $m_a(Q)$ sont deux entiers naturels. Par définition de la multiplicité, il existe P_1 et Q_1 deux polynômes tels que $P = (X-a)^{m_a(P)}P_1$, $Q = (X-a)^{m_a(Q)}Q_1$, $P_1(a) \neq 0$ et $Q_1(a) \neq 0$.

• Pour la première relation, il suffit d'écrire que :

$$PQ = (X-a)^{m_a(P)+m_a(Q)}P_1Q_1 \quad \text{avec } \left(P_1Q_1\right)(a) \neq 0$$

Par suite, $m_a(PQ) = m_a(P) + m_a(Q)$.

• Pour la seconde, en posant $m = \min\left(m_a(P), m_a(Q)\right)$, on a :

$$P + Q = (X-a)^m \times \left((X-a)^{m_a(P)-m}P_1 + (X-a)^{m_a(Q)-m}Q_1\right)$$

On obtient alors le résultat en appliquant la première relation. ⊠

7.4.4 Méthodes pour montrer que deux polynômes sont égaux

Dans de nombreuses situations, on est amené à démontrer que deux polynômes P et Q sont égaux. Il est donc important de bien avoir à l'esprit les différentes méthodes que l'on peut utiliser. La première remarque est que $P = Q$ si et seulement si $P - Q = 0$. Par suite, on s'intéresse aux différentes méthodes pour montrer qu'un polynôme est nul.

► Méthode :

Pour montrer qu'un polynôme P est nul, on peut :

1. montrer que tous ses coefficients sont nuls ;
2. montrer que $\deg(P) < 0$;
3. montrer que P admet strictement plus de racines (comptées avec multiplicités) que son degré ;
4. montrer que P admet une infinité de racines ;
5. montrer qu'il existe $a \in \mathbb{K}$ tel que :

$$\forall k \in [\![0, \deg(P)]\!],\ P^{(k)}(a) = 0$$

7.4.5 Polynômes scindés et relations entre racines et coefficients

Définition 7.4.5.1 On dit qu'un polynôme non constant P est :

- scindé dans $\mathbb{K}$ (ou sur $\mathbb{K}$) s'il admet autant de racines (comptées avec multiplicités) que son degré ;
- scindé à racines simples (ou scindé simple) si P est scindé et toutes les racines de P sont simples, c'est-à-dire de multiplicité 1.

Exemple 7.4.5.2

- X^2-1 est scindé à racines simples dans $\mathbb{R}$ car $X^2-1=(X-1)(X+1)$;
- $P=X^3-2X^2+X$ est scindé dans $\mathbb{R}$ car $P=X(X-1)^2$ mais il n'est pas scindé à racines simples ;
- X^2+1 est scindé à racines simples dans $\mathbb{C}$ mais il n'est pas scindé dans $\mathbb{R}$.

Remarques : *en clair, un polynôme est scindé dans $\mathbb{K}$ s'il peut s'écrire dans $\mathbb{K}[X]$ sous la forme $P=\lambda\prod_{k=1}^{p}(X-a_k)^{m_k}$ où $\lambda\in\mathbb{K}^\star$, les $a_k\in\mathbb{K}$ sont deux à deux distincts, et $m_k\in\mathbb{N}^\star$ est la multiplicité de a_k dans P. On peut aussi reformuler en disant qu'un polynôme est scindé s'il se factorise complètement en produit de puissances de polynômes du premier degré.*

Proposition 7.4.5.3 *On a déjà vu que si $P=aX^2+bX+c$ (avec $a\neq 0$) est scindé dans $\mathbb{K}$, de racines x_1 et x_2 (éventuellement confondues), alors :*

$$x_1+x_2=-\frac{b}{a} \qquad \text{et} \qquad x_1x_2=\frac{c}{a}$$

Proposition 7.4.5.4 *Soit $P=a_3X^3+a_2X^2+a_1X+a_0$ (avec $a_3\neq 0$) scindé dans $\mathbb{K}$ et soient x_1,x_2,x_3 ses racines (comptées avec leur multiplicité), alors :*

$$x_1+x_2+x_3=-\frac{a_2}{a_3} \quad ; \quad x_1x_2+x_1x_3+x_2x_3=\frac{a_1}{a_3} \quad ; \quad x_1x_2x_3=-\frac{a_0}{a_3}$$

Réciproquement, si $x_1,x_2,x_3\in\mathbb{K}$ vérifient les trois relations précédentes, alors ce sont les racines (comptées avec multiplicité) du polynôme $P=a_3X^3+a_2X^2+a_1X+a_0$.

Preuve :

Il suffit de développer le produit $a_3(X-x_1)(X-x_2)(X-x_3)$.

⊠

Remarque : *plus généralement, si $P = a_nX^n + \cdots + a_1X + a_0$ (avec $a_n \neq 0$) est scindé dans $\mathbb{K}$ alors :*

$$\sum_{k=1}^{n} x_k = -\frac{a_{n-1}}{a_n} \qquad et \qquad \prod_{k=1}^{n} x_k = (-1)^n \frac{a_0}{a_n}$$

On peut aussi retrouver les autres coefficients à l'aide des fonctions symétriques élémentaires :

$$\sigma_k = \sum_{1 \leqslant i_1 < i_2 \cdots < i_k \leqslant n} x_{i_1} \times \cdots \times x_{i_k} = (-1)^k \frac{a_{n-k}}{a_n}$$

Et réciproquement, si les nombres $x_1, \cdots, x_n$ (non nécessairement distincts) vérifient :

$$\forall k \in [\![1, n]\!] \ , \ \sigma_k = (-1)^k \frac{a_{n-k}}{a_n}$$

alors ce sont les racines (comptées avec multiplicité) du polynôme $P = \sum_{k=0}^{n} a_k X^k$.

Preuve :

À nouveau, il suffit de développer l'expression :

$$a_n \prod_{k=1}^{n} (X - x_k) = a_n \sum_{k=0}^{n} (-1)^{n-k} \sigma_{n-k} X^k$$

⊠

Exercice 7.4.5.5 Déterminer l'ensemble des réels p tels que le système

$$(S) : \begin{cases} x + y + z &= 2 \\ xy + xz + yz &= 1 \\ xyz &= p \end{cases}$$

admette au moins une solution dans $\mathbb{R}^3$.

Corollaire 7.4.5.6 *Soient A et B deux polynômes tel que A est scindé dans $\mathbb{K}$. Alors $A|B$ si et seulement si pour tout $a \in \mathbb{K}$, $m_a(A) \leqslant m_a(B)$.*

7.5 Polynômes irréductibles et factorisation

Rappel : un polynôme $P \in \mathbb{K}[X]$ est irréductible dans $\mathbb{K}[X]$ si $\deg P \geqslant 1$ et si les seuls diviseurs de P sont les unités (c'est-à-dire les polynômes constants non nuls) ou les polynômes associés à P. Autrement dit, P est irréductible si $\deg(P) \geqslant 1$ et :

$$\forall (Q,R) \in \mathbb{K}[X]^2 \ , \ (P = QR \Longrightarrow Q \in \mathbb{K}^\star \quad \text{ou} \quad R \in \mathbb{K}^\star)$$

Théorème 7.5.0.1 *Tout polynôme de degré $n \geqslant 1$, se factorise de façon unique (à l'ordre près) en produit de polynômes irréductibles et unitaires et d'une unité de $\mathbb{K}[X]$.*

Preuve :

• Pour l'existence, on procède par récurrence forte sur $\deg P$.

Initialisation :

Pour $n = 1$, c'est évident car tout polynôme du premier degré est irréductible. Donc si $P = aX + b$ avec $a \neq 0$, $P = a(X - \frac{b}{a})$ est le produit d'une unité ($a \in \mathbb{K}^\star$) et d'un polynôme irréductible et unitaire.

Hérédité :

On suppose la propriété vraie jusqu'au rang $n \geqslant 1$: montrons qu'elle est vraie au rang $n+1$. Soit P de degré $n+1$.

- ∗ Si P est irréductible, c'est fini : en notant $\lambda \in \mathbb{K}^\star$ le coefficient dominant de P, on a : $P = \lambda \frac{P}{\lambda}$ avec $\frac{P}{\lambda}$ irréductible et unitaire ;
- ∗ sinon, il existe deux polynômes non constants Q et R tels que $P = QR$. On applique alors l'hypothèse de récurrence à Q et R.

Ce qui prouve que la propriété est vraie au rang $n+1$ et achève la récurrence.

• On admet l'unicité à l'ordre près. Pour les plus courageux, vous pouvez le démontrer : c'est un peu technique mais l'outil essentiel est le même que dans $\mathbb{Z}$: c'est le lemme d'Euclide.

⊠

Remarques : *on dispose alors des mêmes méthodes que dans $\mathbb{Z}$.*

- *Pour montrer que $A|B$ dans $\mathbb{K}[X]$, il faut et il suffit de montrer que pour chaque facteur irréductible P de A, $m_P(A) \leqslant m_P(B)$ (c'est-à-dire que la multiplicité de P dans A est inférieure à la multiplicité de P dans B).*

- *Si* $A = \lambda \prod_{i=1}^{n} P_i^{\alpha_i}$ *et* $B = \mu \prod_{i=1}^{n} P_i^{\beta_i}$ *avec* $n \in \mathbb{N}^\star$, $\lambda, \mu \in \mathbb{K}^\star$, *pour tout* $i \in [\![1, n]\!]$, P_i *unitaire et irréductible,* $\alpha_i, \beta_i \in \mathbb{N}$, *et les* P_i *deux à deux distincts, alors :*

$$pgcd(A, B) = \prod_{i=1}^{n} P_i^{\min(\alpha_i, \beta_i)} \quad et \quad ppcm(A, B) = \prod_{i=1}^{n} P_i^{\max(\alpha_i, \beta_i)}$$

7.5.1 Éléments irréductibles dans $\mathbb{C}[X]$

Le théorème suivant est souvent appelé théorème fondamental de l'algèbre. Ce théorème est admis mais une démonstration est proposée en exercice.

Théorème 7.5.1.1 (théorème de D'Alembert-Gauss) *Tout polynôme* $P \in \mathbb{C}[X]$ *non constant admet au moins une racine dans* $\mathbb{C}$.

Remarque : *on dit aussi que le corps* $\mathbb{C}$ *est algébriquement clos.*

Corollaire 7.5.1.2 *Les polynômes irréductibles dans* $\mathbb{C}[X]$ *sont les polynômes du premier degré.*

Corollaire 7.5.1.3 *Tout polynôme* $P \in \mathbb{C}[X]$ *non constant est scindé dans* $\mathbb{C}$.

Preuve du premier corollaire :

• Tout d'abord, on a déjà vu qu'un polynôme de degré un est irréductible.

• Réciproquement, soit $P \in \mathbb{C}[X]$ un polynôme irréductible. Alors, par définition $\deg(P) \geqslant 1$. D'après le théorème de D'Alembert-Gauss, P admet au moins une racine complexe α et $(X - \alpha)$ divise P. Or, P est irréductible et $X - \alpha$ n'est pas constant. Par suite, $X - \alpha$ et P sont associés et par conséquent, P est un polynôme de degré 1. ⊠

Preuve du second corollaire :

Montrons par récurrence sur $n \geqslant 1$ que tout polynôme de degré n est scindé dans $\mathbb{C}$.

Initialisation :
Pour $n = 1$, c'est clair.

Hérédité :

On suppose que la propriété est vraie au rang $n \geqslant 1$ et on montre qu'elle est vraie au rang $n+1$. Soit $P \in \mathbb{C}[X]$ de degré $n+1$. Alors P admet au moins une racine α et il existe alors $Q \in \mathbb{C}[X]$ tel que $P = (X-\alpha)Q$. De plus, $\deg Q = n$ donc d'après l'hypothèse de récurrence, Qest scindé dans $\mathbb{C}$ et donc P l'est aussi.

⊠

7.5.2 Éléments irréductibles dans $\mathbb{R}[X]$

Théorème 7.5.2.1 *Les polynômes irréductibles dans $\mathbb{R}[X]$ sont :*

(i) les polynômes de degré 1 ;

(ii) les polynômes du second degré dont le discriminant est strictement négatif.

Preuve :

• Tout d'abord, il est clair qu'il s'agit bien de polynômes irréductibles dans $\mathbb{R}[X]$.

• Réciproquement, montrons que ce sont les seuls. Soit $P \in \mathbb{R}[X]$ irréductible de degré supérieur ou égal à 2. Alors P n'a pas de racine réelle (sinon on peut le factoriser par $X-a$ et il n'est pas irréductible). D'après le théorème de D'Alembert-Gauss, P admet au moins une racine complexe α. P étant à coefficients réels, on a alors $P(\overline{\alpha}) = \overline{P(\alpha)} = 0$. Ainsi, $\alpha \neq \overline{\alpha}$ et on peut factoriser P par $(X-\alpha)(X-\overline{\alpha}) = X^2 - 2\Re e(\alpha)X + |\alpha|^2 \in \mathbb{R}[X]$. On a donc trouvé un diviseur non constant de P. Celui-ci étant supposé irréductible, $P = \lambda(X^2 - 2\Re e(\alpha)X + |\alpha|^2)$ avec $\lambda \in \mathbb{R}^\star$.

⊠

Corollaire 7.5.2.2 *Tout polynôme $P \in \mathbb{R}[X]$ non constant s'écrit de façon unique à l'ordre près sous la forme :*

$$P = \lambda \times \prod_{k=1}^{r} (X-\alpha_k)^{m_k} \times \prod_{k=1}^{s} (X^2 + b_k X + c_k)^{n_k}$$

où $\lambda \in \mathbb{R}^\star$, $r, s \in \mathbb{N}$ (non tous deux nuls), pour $1 \leqslant k \leqslant r$, $\alpha_k \in \mathbb{R}$ et deux à deux distincts, $m_k \in \mathbb{N}^\star$, pour $1 \leqslant k \leqslant s$, $(b_k, c_k) \in \mathbb{R}^2$ deux à deux distincts, $n_k \in \mathbb{N}^\star$, $b_k^2 - 4c_k < 0$.

Exemple 7.5.2.3 Déterminons la décomposition en facteurs irréductibles dans $\mathbb{R}[X]$ du polynôme $P = X^4 + 1$.

Déjà, P n'a pas de racine dans $\mathbb{R}$ mais on sait qu'il n'est pas irréductible puisqu'il est de degré 4. Pour le factoriser, on utilise la méthode usuelle : on le factorise dans $\mathbb{C}[X]$ puis on regroupe les racines complexes conjuguées.

Soit $z \in \mathbb{C}$. $z^4 + 1 = 0 \iff z^4 = -1 \iff z = i^k e^{i\frac{\pi}{4}}$ avec $0 \leqslant k \leqslant 3$. On a alors :

$$X^4 + 1 = (X - e^{i\frac{\pi}{4}})(X - e^{i\frac{3\pi}{4}})(X - e^{i\frac{5\pi}{4}})(X - e^{i\frac{7\pi}{4}}) \quad \text{(factorisation dans } \mathbb{C}[X])$$

Or,

$$(X - e^{i\frac{\pi}{4}})(X - e^{i\frac{7\pi}{4}}) = (X - e^{i\frac{\pi}{4}})(X - e^{-i\frac{\pi}{4}}) = X^2 - \sqrt{2}X + 1$$

et de la même façon,

$$(X - e^{i\frac{3\pi}{4}})(X - e^{i\frac{5\pi}{4}}) = X^2 + \sqrt{2}X + 1$$

D'où l'on déduit la décomposition en facteurs irréductibles dans $\mathbb{R}[X]$:

$$P = (X^2 - \sqrt{2}X + 1)(X^2 + \sqrt{2}X + 1) \quad \text{(factorisation dans } \mathbb{R}[X])$$

Exercice 7.5.2.4 Donner les décompositions dans $\mathbb{C}[X]$ puis dans $\mathbb{R}[X]$ des polynômes $P = X^n - 1$ et $Q = X^n + 1$. *On pourra distinguer les cas n pair et n impair.*

7.6 Ensemble $\mathbb{K}(X)$

7.6.1 Corps des fractions rationnelles $\mathbb{K}(X)$

Définition 7.6.1.1 On appelle fraction rationnelle à une indéterminée et à coefficients dans $\mathbb{K}$ toute expression formelle de la forme $F = \frac{A}{B}$ où $A, B \in \mathbb{K}[X]$ et $B \neq 0$. On dit alors que $\frac{A}{B}$ est un représentant de la fraction rationnelle F.

L'ensemble des fractions rationnelles à une indéterminée et à coefficients dans $\mathbb{K}$ est noté $\mathbb{K}(X)$.

Définition 7.6.1.2 On dit que deux fractions rationnelles $F = \frac{A}{B}$ et $G = \frac{C}{D}$ sont égales si $AD = BC$.

Théorème 7.6.1.3 (Admis) *On munit $\mathbb{K}(X)$ de deux lois de compostions internes $+$ et $\times$, et d'une multiplication externe notée $\cdot$, définies respectivement par :*

$$\forall A, C \in \mathbb{K}[X]\ ,\ \forall B, D \in \mathbb{K}[X] \setminus \{0\}\ ,\ \forall \lambda \in \mathbb{K}\ ,\ \frac{A}{B} + \frac{C}{D} = \frac{AD + BC}{BD}\ ;$$

$$\frac{A}{B} \times \frac{C}{D} = \frac{A \times C}{B \times D} \text{ et } \lambda \cdot \frac{A}{B} = \frac{\lambda \cdot A}{B}$$

Alors :

(i) les lois $+$, $\times$ et $\cdot$ sont bien définies, c'est-à-dire ne dépendent pas du choix des représentants des fractions rationnelles ;

(ii) $(\mathbb{K}(X), +, \times)$ est un corps commutatif ;

(iii) $(\mathbb{K}(X), +, \cdot)$ est un $\mathbb{K}$-espace vectoriel ;

(iv) L'application $\psi : \mathbb{K}[X] \longrightarrow \mathbb{K}(X)$ qui à A associe $\frac{A}{1}$ est un morphisme d'algèbres qui est injectif. Ceci permet d'identifier un polynôme A avec la fraction rationnelle $\frac{A}{1}$. Ainsi, $\mathbb{K}[X]$ est une sous-$\mathbb{K}$-algèbre de $\mathbb{K}(X)$.

Définition 7.6.1.4 Soit $F \in \mathbb{K}(X) \setminus \{0\}$. On appelle représentant irréductible de F toute fraction $F = \frac{A}{B}$ avec $(A, B) \in (\mathbb{K}[X] \setminus \{0\})^2$ tel que $A \wedge B = 1$.

Remarque : *en fait, c'est le même principe que pour le passage de $\mathbb{Z}$ à $\mathbb{Q}$. On simplifie au maximum la fraction : une fois simplifiée, on obtient un représentant irréductible. Par exemple,*

$$F = \frac{X^3 + 2X^2 + X}{X^4 + 3X^3 + 2X^2} = \frac{X(X+1)^2}{X^2(X+1)(X+2)} = \frac{X+1}{X(X+2)}$$

La fraction $\dfrac{X+1}{X(X+2)}$ est irréductible : c'est donc un représentant irréductible de F.

7.6.2 Dérivation et degré

Définition 7.6.2.1 On définit pour $F = \frac{A}{B}$ avec $A, B \in \mathbb{K}[X]$ et $B \neq 0$,

$$\deg(F) = \deg(A) - \deg(B)$$

Proposition 7.6.2.2 *On considère l'application* deg $: \mathbb{K}(X) \longrightarrow \mathbb{Z} \cup \{-\infty\}$.

(i) L'application deg *est bien définie, c'est-à-dire que le degré d'une fraction rationnelle ne dépend pas du choix du représentant de la fraction rationnelle.*

(ii) Cette nouvelle application deg *prolonge l'application* deg *définie sur* $\mathbb{K}[X]$.

(iii) Pour tout $(F, G) \in \mathbb{K}(X)^2$ *et tout* $\lambda \in \mathbb{K}^\star$,

$$\deg(F \times G) = \deg(F) + \deg(G) \ ; \ \deg(\lambda \cdot F) = \deg(F) \ ;$$

$$\deg(F + G) \leqslant \max(\deg(F), \deg(G))$$

Preuve :

• Pour (i), il suffit de remarquer que si $\frac{A}{B} = \frac{C}{D}$, avec $A, B, C, D \in \mathbb{K}[X]$, $B \neq 0$ et $D \neq 0$, alors $AD = BC$. Par suite,

$$\deg(A) + \deg(D) = \deg(B) + \deg(C)$$

c'est-à-dire

$$\deg(A) - \deg(B) = \deg(C) - \deg(D)$$

• Pour (ii), si $A \in \mathbb{K}[X]$, alors $A = \frac{A}{1}$ et :

$$\deg(\frac{A}{1}) = \deg(A) - \deg(1) = \deg(A)$$

donc le degré de A en tant que fraction rationnelle est le même que le degré de A en tant que polynôme.

• Enfin, pour (iii), les deux premières relations sont évidentes. Pour la troisième, on constate que si $F = \frac{A}{B}$ et $G = \frac{C}{D}$ avec $B \neq 0$ et $D \neq 0$, alors :

$$\deg(F + G) = \deg\left(\frac{AD + BC}{BD}\right) = \deg(AD + BC) - \deg(BD)$$

Or, d'une part, $\deg(AD + BC) \leqslant \max(\deg(AD), \deg(BC))$ et d'autre part, $\max(\deg(AD), \deg(BC)) = \max(\deg(A)+\deg(D), \deg(B)+\deg(C))$. Donc, en notant $m = \deg(AD + BC) - \deg(BD)$, on a :

$$\begin{aligned} m &\leqslant \max(\deg(A)+\deg(D)-\deg(BD), \deg(B)+\deg(C)-\deg(BD)) \\ &\leqslant \max(\deg(A) - \deg(B), \deg(C) - \deg(D)) \\ &\leqslant \max(\deg(F), \deg(G)) \end{aligned}$$

⊠

Exemple 7.6.2.3 Si $F = \dfrac{X}{X^2+1}$, alors $\deg(F) = 1 - 2 = -1$.

Définition 7.6.2.4 Soit $F \in \mathbb{K}(X)$ et soient $A, B \in \mathbb{K}[X]$ tels que $B \neq 0$ et $F = \dfrac{A}{B}$. On définit la dérivée de F, notée $D(F)$ ou encore F', par :

$$D(F) = \frac{A'B - AB'}{B^2}$$

Proposition 7.6.2.5 (Admis) *L'application $D : \mathbb{K}(X) \longrightarrow \mathbb{K}(X)$ qui à F associe $D(F)$ est bien définie et prolonge la dérivation sur l'ensemble des polynômes.*
De plus, les formules usuelles de dérivation restent valables, c'est-à-dire que pour toutes fractions rationnelles F et G et toute constante $\lambda \in \mathbb{K}$, on a :

$$D(F+G) = D(F) + D(G) \ ; \ D(F \times G) = FD(G) + FD(G) \ ; \ D(\lambda D) = \lambda D(F) \ ;$$

$$D\left(\frac{F}{G}\right) = \frac{D(F)G - FD(G)}{G^2}$$

7.6.3 Zéros et pôles d'une fraction rationnelle

Définition 7.6.3.1 Soit $F \in \mathbb{K}(X) \setminus \{0\}$ et soit $\frac{A}{B}$ une représentation irréductible de F, avec $A, B \in \mathbb{K}[X] \setminus \{0\}$.

- On appelle zéro de F toute racine $a \in \mathbb{K}$ de A. Dans ce cas, on appelle ordre de multiplicité du zéro a de F la multiplicité de la racine a dans A.
- On appelle pôle de F toute racine $a \in \mathbb{K}$ du polynôme B. Dans ce cas, on appelle ordre de multiplicité du pôle a de F la multiplicité de a en tant que racine de B.

Exemple 7.6.3.2 Soit $F = \dfrac{X^4(X+1)^2}{X^2(X+1)^5(X-2)}$. Une représentation irréductible de F est alors :

$$F = \frac{X^2}{(X+1)^3(X-2)}$$

Par conséquent,

- F a un seul zéro qui est 0 et son ordre de multiplicité est 2 ;
- F a deux pôles : -1 et 2 qui ont pour ordre de multiplicité 3 et 1 respectivement.

7.6.4 Décomposition en éléments simples

Définition 7.6.4.1 On appelle éléments simples de $\mathbb{K}(X)$:

- les monômes de $\mathbb{K}[X]$;
- les éléments de $\mathbb{K}(X)$ de la forme : $\dfrac{A}{P^n}$ où $P \in \mathbb{K}[X]$ est irréductible, $n \in \mathbb{N}^\star$, $A \in \mathbb{K}[X] \setminus \{0\}$ et $\deg(A) < \deg(P)$.

Exemple 7.6.4.2 Les éléments simples de $\mathbb{C}(X)$ sont les monômes et les éléments de la forme :

$$\frac{a}{(X-\alpha)^n} \qquad \text{avec } a \in \mathbb{C}^\star \text{ , } \alpha \in \mathbb{C} \text{ et } n \in \mathbb{N}^\star$$

Exemple 7.6.4.3 Dans $\mathbb{R}(X)$, les éléments simples sont les monômes et les éléments de la forme :

$$\frac{a}{(X-\alpha)^n} \quad \text{ou bien} \quad \frac{cX+d}{(X^2-ex+f)^m}$$

avec $a \in \mathbb{R}^\star$, $\alpha \in \mathbb{R}$, $n \in \mathbb{N}^\star$, $(c,d) \in \mathbb{R}^2 \setminus \{(0,0)\}$, $(e,f) \in \mathbb{R}^2$ et $e^2 - 4f < 0$ et $m \in \mathbb{N}^\star$.

Théorème 7.6.4.4 (Décomposition en éléments simples) *Toute fraction rationnelle se décompose de façon unique en combinaison linéaire d'éléments simples.*

Plus exactement, si $F = \frac{A}{\prod_{i=1}^{N} P_i^{n_i}}$ *avec* $A \in \mathbb{K}[X]$, $N \in \mathbb{N}$, $P_1, \cdots, P_N$ *irréductibles et premiers entre eux deux à deux et* $n_1, \cdots, n_N \in \mathbb{N}^\star$, *alors il existe une unique famille de polynômes* $(E, C_{1,1}, C_{2,1}, \cdots, C_{n_1,1}, C_{1,2}, \cdots, C_{n_2,2}, \cdots, C_{1,N}, \cdots C_{n_N,N})$ *telle que :*

$$\begin{cases} F = E + \displaystyle\sum_{i=1}^{N} \sum_{j=1}^{n_i} \frac{C_{j,i}}{P_i^j} \\ \\ \forall i \in [\![1, N]\!] \text{ , } \forall j \in [\![1, n_i]\!] \text{ , } \deg(C_{j,i}) < \deg(P_i) \end{cases}$$

E est appelée la partie entière (ou principale) de F.

On admet ce théorème. Ce qui compte c'est de savoir l'appliquer. Pour cela, on va traiter quelques exemples.

Exemple 7.6.4.5 Soit $F = \dfrac{X^3+X-1}{X^2-1}$. Pour commencer, on détermine la partie entière de F. Celle-ci est obtenue comme le quotient de la division euclidienne de X^3+X-1 par X^2-1. Le calcul donne :

$$X^3+X-1 = X\times(X^2-1)+2X-1$$

Par suite, $F = X + \dfrac{2X-1}{X^2-1}$. Ensuite, $X^2-1=(X-1)(X+1)$ et c'est la décomposition en facteurs irréductibles. D'après le théorème de décomposition en éléments simples :

$$\frac{2X-1}{X^2-1} = \frac{a}{X-1}+\frac{b}{X+1} \quad \text{avec } (a,b)\in\mathbb{R}^2$$

En identifiant, on trouve $a=\frac{1}{2}$ et $b=\frac{3}{2}$. Par conséquent, la décomposition en éléments simples de F est :

$$F = X+\frac{1/2}{X-1}+\frac{3/2}{X+1}$$

Exemple 7.6.4.6 Soit $G = \dfrac{X+1}{X^3(X-1)^2}$. Puisque $\deg(G)<0$, la partie entière de G est nulle. Le théorème de décomposition en éléments simples permet de dire qu'il existe $(a,b,c,d,e)\in\mathbb{R}^5$ (qui est unique) tel que :

$$G = \frac{a}{X}+\frac{b}{X^2}+\frac{c}{X^3}+\frac{d}{X-1}+\frac{e}{(X-1)^2}$$

Il reste alors à calculer les valeurs de a,b,c,d et e ! Puisqu'on sait que la décomposition existe et est unique, on peut utiliser toute méthode (qui est juste) pour déterminer les nombres en question.

Par exemple, $\tilde{G}(x) \underset{x\to 1}{\sim} \dfrac{2}{(x-1)^2}$. Ce qui permet directement de conclure que $e=2$ puisque :

$$\frac{a}{x}+\frac{b}{x^2}+\frac{c}{x^3}+\frac{d}{x-1}+\frac{e}{(x-1)^2} \underset{x\to 1}{=} \frac{e}{(x-1)^2}+o\left(\frac{1}{(x-1)^2}\right)$$

De façon similaire,

$$\tilde{G}(h) \underset{h\to 0}{=} \frac{1}{h^3}\frac{1+h}{(1-h)^2} \underset{h\to 0}{=} \frac{1}{h^3}\left(1+3h+5h^2+o(h^2)\right)$$

Ce qui permet de conclure que $c=1$, $b=3$ et $a=5$ (unicité du développement limité de $h\longmapsto h^3\tilde{G}(h)$ en 0). Enfin, $\tilde{G}(x) \underset{x\to+\infty}{=} o(\frac{1}{x})$ implique que $a+d=0$, donc $d=-a=-5$.

Exercice 7.6.4.7 Déterminer la décomposition en éléments simples dans $\mathbb{R}[X]$ de

$$H = \frac{X}{(X-1)(X^2+1)^2}$$

7.7 Exercices

Exercice 7.7.1 Quels sont les degrés et coefficients dominants des polynômes suivants :

$$(X+1)^n-(X-1)^n \quad ; \quad (X^2+1)^n-(X^2-1)^n$$

Exercice 7.7.2 Montrer que pour tout entier naturel non nul n :

$$(X^3+X^2+X+1)\sum_{k=0}^{2n}(-1)^k X^k = X^{2n+3}+X^{2n+1}+X^2+1$$

Exercice 7.7.3 Soient $n\in\mathbb{N}^\star$ et $(a_0,\cdots,a_n)\in\mathbb{K}^{n+1}$. On considère les polynômes :

$$\begin{aligned} P &= a_0+a_1X+a_2X(X-1)+\cdots+a_nX(X-1)\cdots(X-n+1)\\ Q &= a_0+\frac{a_1}{2}X(X-1)+\cdots+\frac{a_n}{2^n}X(X-1)\cdots(X-n+1)\end{aligned}$$

1. Pour $k\in\mathbb{N}$, exprimer $P(k)$ sous forme d'une somme avec coefficients binomiaux.
2. En déduire que $\displaystyle\sum_{k=0}^{n}\binom{n}{k}P(k)=\sum_{j=0}^{n}a_j\sum_{k=j}^{n}\frac{n!}{(n-k)!(k-j)!}$.
3. Conclure que $\displaystyle\sum_{k=0}^{n}\binom{n}{k}P(k)=\sum_{j=0}^{n}a_j\frac{n!}{(n-j)!}2^{n-j}=2^nQ(n)$.

Exercice 7.7.4 Résoudre les équations suivantes dans $\mathbb{K}[X]$:

$$Q^2=XP^2 \quad ; \quad P'^2=4P \quad ; \quad P'P''=18P$$

Exercice 7.7.5 Soit Δ l'application définie par : $\begin{array}{ccc}\mathbb{K}[X] & \longrightarrow & \mathbb{K}[X]\\ P & \longmapsto & P(X+1)-P(X)\end{array}$

1. Montrer que $\Delta\in\mathcal{L}(\mathbb{K}[X])$.
2. Soit $n\geqslant 1$ un entier donné. Démontrer que $\Delta(\mathbb{K}_n[X])\subset\mathbb{K}_{n-1}[X]$.
3. En déduire que si $\deg P<n$, alors $\Delta^n(P)=0$.
4. Prouver que si $P\in\mathbb{K}[X]$ et $\deg P<n$, alors : $\displaystyle\sum_{k=0}^{n}(-1)^k\binom{n}{k}P(k)=0$.

Exercice 7.7.6 Effectuer la division euclidienne de :

1. $X^6-4X^3+2X^2-1$ par X^2+4.
2. $4X^3+X^2$ par $X+1+i$.
3. iX^3-X^2 par $(1+i)X^2-iX+3$.

Exercice 7.7.7 Déterminer le reste de la division euclidienne de P par $(X-a)(X-b)$ lorsque $a\neq b$. Comment modifier ce résultat lorsque $a=b$?

Exercice 7.7.8 Soit $P \in \mathbb{K}[X]$ tel que les restes de la division euclidienne de P par X^2+1 et X^2-1 sont respectivement $2X-2$ et $-4X$. Quel est le reste de la division euclidienne de P par X^4-1 ?

Exercice 7.7.9 Quel est le reste de la division euclidienne de $(X\sin\theta+\cos\theta)^n$ par X^2+1, où $\theta \in \mathbb{R}$ et $n \in \mathbb{N}$?

Exercice 7.7.10 Soit $P \in \mathbb{R}[X]$. Montrer que $P(X) = P(1-X)$ si et seulement si toutes les dérivées d'ordre impair de P s'annulent en $\dfrac{1}{2}$.

Exercice 7.7.11 Soit le polynôme $P = X^6 - 5X^4 + 8X^3 - 9X^2 + aX + b$ où a et b sont, pour l'instant, deux réels quelconques.

1. Montrer que 1 est une racine multiple de P si et seulement si $a = 8$ et $b = -3$.
   Dans toute la suite de l'exercice, on suppose que $a = 8$ et $b = -3$.
2. Montrer que 1 est alors racine de P de multiplicité égale à 3.
3. Vérifier ce résultat en effectuant la division euclidienne de P par $(X-1)^3$. Préciser la valeur du quotient Q.
4. Factoriser Q en produit de polynômes irréductibles dans $\mathbb{R}[X]$ puis dans $\mathbb{C}[X]$.
5. En déduire la factorisation de P en produit de polynômes irréductibles dans $\mathbb{R}[X]$ et dans $\mathbb{C}[X]$.
6. Factoriser le polynôme X^4+1 en produit de facteurs irréductibles dans $\mathbb{C}[X]$ puis dans $\mathbb{R}[X]$.
7. En déduire la factorisation de $P(X^2)$ en produit de polynômes irréductibles dans $\mathbb{R}[X]$ et dans $\mathbb{C}[X]$.
8. Décomposer $\dfrac{1}{(X+3)(X^2+1)}$ en éléments simples dans $\mathbb{C}[X]$ puis dans $\mathbb{R}[X]$.

Exercice 7.7.12 Montrer que $X^3 + pX + q$ admet une racine multiple si et seulement si $4p^3 + 27q^2 = 0$.

Exercice 7.7.13

1. Montrer qu'il existe une unique suite de polynômes (P_n) telle que :
   $$\forall n \in \mathbb{N}\ ,\ \forall \theta \in \mathbb{R}\ ,\ P_n(\cos(\theta)) = \cos(n\theta)$$
   Ces polynômes sont appelés des polynômes de Tchebychev.
2. Montrer que cette famille vérifie la relation de récurrence :
   $\forall n \in \mathbb{N}\ ,\ P_{n+2} = 2XP_{n+1} - P_n$.
3. En déduire que $P_n \in \mathbb{Z}[X]$ et préciser le degré de P_n ainsi que son coefficient dominant pour tout entier n.
4. Montrer que pour tout entier $n \geqslant 1$, P_n est scindé à racines simples dans $\mathbb{R}$.

Exercice 7.7.14 Soit $P \in \mathbb{R}[X]$ tel que $\forall x \in \mathbb{R}$, $P(x) \geqslant 0$. On veut montrer qu'il existe $A, B \in \mathbb{R}[X]$ tels que : $P = A^2 + B^2$.

1. *Première méthode : par factorisation dans* $\mathbb{C}$.
   (a) Montrer qu'un tel polynôme est nécessairement de degré pair.
   (b) Montrer que si un tel polynôme P admet une racine réelle, alors sa multiplicité est paire.
   (c) Montrer que si α est une racine complexe non réelle de P, alors $\overline{\alpha}$ l'est aussi et possède la même multiplicité.
   (d) En remarquant que $A^2 + B^2 = (A + iB)(A - iB)$, conclure.
2. *Deuxième méthode : par récurrence*

   On utilise les résultats des questions (a) et (b) précédentes.
   (a) Montrer que si $\deg P = 2$, la propriété est vraie.
   (b) Montrer que si $\deg P = 2n + 2$, il existe $U, V \in \mathbb{R}[X]$ tels que $P = UV$, $\deg U = 2$, $\forall x \in \mathbb{R}$, $U(x) \geqslant 0$ et $\forall x \in \mathbb{R}$, $V(x) \geqslant 0$.
   (c) Montrer le résultat par récurrence. *On pourra comparer* $(ac+bd)^2+(ad-bc)^2$ *et* $(a^2+b^2)(c^2+d^2)$.

Exercice 7.7.15 Factoriser dans $\mathbb{R}[X]$ les polynômes suivants ($a \in \mathbb{R} \setminus \pi\mathbb{Z}$) :

X^3-5X^2+3X+9 ; X^5+1 ; $(X^2-X+2)^2+(X-2)^2$; X^8+X^4+1 ; $X^{2n}-2\cos(a)X^n+1$

Exercice 7.7.16 Soit $P \in \mathbb{R}[X]$ tel que $\deg P = n \in \mathbb{N}^\star$ et $\forall k \in [\![1, n+1]\!]$, $P(k) = \dfrac{1}{k}$. Calculer $P(n+2)$.

Exercice 7.7.17 Pour $n \in \mathbb{N}^\star$, on pose $P_n = (X+i)^{2n+1} - (X-i)^{2n+1}$.

1. Déterminer la factorisation en facteurs irréductibles de P_n dans $\mathbb{C}[X]$.
2. En regroupant les facteurs irréductibles par 2 et de façon astucieuse, montrer que pour $a \in \mathbb{C}$ et $n \in \mathbb{N}^\star$:

$$\prod_{k=1}^{n} \left(a^2 + \operatorname{cotan}^2 \left(\frac{k\pi}{2n+1} \right) \right) = \frac{(a+1)^{2n+1} - (a-1)^{2n+1}}{2(2n+1)}$$

Exercice 7.7.18 Donner la multiplicité de 1 pour $X^{2n+1}-(2n+1)X^{n+1}+(2n+1)X^n-1$? Quelle est celle de $a \in \mathbb{C}$ dans $(X-a)(A'+A'(a)) - 2(A-A(a))$?

Exercice 7.7.19 Soient P et Q deux polynômes dans $\mathbb{C}[X]$ non constants. On note $Z(P)$ l'ensemble des racines de P. On suppose que $Z(P) = Z(Q)$ et $Z(P-1) = Z(Q-1)$. On veut montrer que $P = Q$

1. Déterminer une relation entre $|Z(P)|$, $\deg P$ et $\deg(P \wedge P')$.
2. Justifier que l'on peut toujours supposer que $\deg(P) \geqslant \deg(Q)$, ce que l'on fera par la suite.
3. Montrer que $P - Q$ admet au moins $\deg(P) + 1$ racines et conclure.

Exercice 7.7.20 On considère la suite de polynômes définie par :

$$P_0 = 1 \ , \ P_1 = -X \quad \text{et} \quad \forall n \in \mathbb{N} \ , \ P_{n+2} + XP_{n+1} + P_n = 0$$

1. Déterminer le degré et le coefficient dominant de P_n.
2. Calculer $P_n(0)$ pour $n \in \mathbb{N}$.
3. Étudier la parité de P_n.
4. On fixe $x \in]-2, 2[$.
   (a) Montrer qu'il existe un unique $\theta \in]0, \pi[$ tel que $x = 2\cos(\theta)$.
   (b) On pose pour $n \in \mathbb{N}$, $u_n = P_n(2\cos(\theta))$. Montrer que (u_n) est une suite récurrente linéaire d'ordre 2.
   (c) En déduire l'expression de u_n en fonction de n et θ.
   (d) Montrer alors que pour tout entier n, P_n est scindé dans $\mathbb{R}$ et donner les racines de P_n.
5. En considérant les racines de P_{2n}, calculer pour $n \in \mathbb{N}$, $A_n = \prod_{k=1}^{n} \cos\left(\frac{k\pi}{2n+1}\right)$.

Exercice 7.7.21 Soit $n \in \mathbb{N}$. On se donne $x_0, \cdots, x_n \in \mathbb{K}$ deux à deux distincts.

1. Soit $i \in [\![0, n]\!]$ fixé. Montrer qu'il existe un unique polynôme L_i vérifiant :

$$\deg L_i \leqslant n \quad ; \quad \forall j \in [\![0, n]\!] \setminus \{i\} \ , L_i(x_j) = 0 \quad ; \quad L_i(x_i) = 1$$

2. En déduire que si $(b_0, b_1, \cdots, b_n) \in \mathbb{K}^{n+1}$, il existe un unique polynôme de degré inférieur ou égal à n vérifiant :

$$\forall i \in [\![0, n]\!] \, , \, P(x_i) = b_i$$

   Remarque : les polynômes L_i sont appelés polynômes d'interpolation de Lagrange aux points $x_0, \cdots, x_n$.

3. Application : soit $P \in \mathbb{C}[X]$ tel que $P(\mathbb{Q}) \subset \mathbb{Q}$. Montrer que $P \in \mathbb{Q}[X]$.

Exercice 7.7.22 Déterminer la décomposition en éléments simples des fractions rationnelles suivantes :

$$F = \frac{X^2+1}{X(X-1)(X-2)} \ ; \ G = \frac{1}{X^2(X-1)^3} \ ; \ H = \frac{2X}{(X^2+1)^2(X^2-1)}$$

Exercice 7.7.23 Soit $n \geqslant 1$. Déterminer explicitement la décomposition en éléments simples de $\dfrac{1}{(X^2-1)^n}$.

Exercice 7.7.24 Le but de l'exercice est de démontrer le théorème de D'Alembert-Gauss.

1. Rappeler l'énoncé de ce théorème.
2. Soit f une fonction de $\mathbb{C}$ dans $\mathbb{C}$.
   (a) Pour $a \in \mathbb{C}$, donner la définition de f continue en a.
   (b) Montrer que si f est continue sur $\overline{B}(a,R) = \{z \in \mathbb{C} \ , \ |z-a| \leqslant R\}$, avec $R > 0$, alors f est bornée et atteint ses bornes, c'est-à-dire qu'il existe $z_1, z_2 \in \overline{B}(a,R)$ tels que :
   $$|f(z_1)| = \inf_{z \in \overline{B}(a,R)} |f(z)| \quad \text{et} \quad |f(z_2)| = \sup_{z \in \overline{B}(a,R)} |f(z)|$$
3. Soient $P \in \mathbb{C}[X]$ non constant, $n = \deg P$ et a_n le coefficient dominant de P. On suppose que P n'a pas de racine complexe.
   (a) Montrer que $|P(z)| \underset{|z| \to +\infty}{\sim} |a_n||z|^n$.
   (b) En déduire qu'il existe $R > 0$ tel que : $\forall z \in \mathbb{C} \ , \ (|z| > R \Longrightarrow |P(z)| \geqslant |P(0)|)$.
   (c) Prouver qu'il existe $z_0 \in \mathbb{C}$ tel que : $|P(z_0)| = \inf_{z \in \mathbb{C}} |P(z)|$.
   (d) Justifier l'existence de $p = \min\{k \in [\![1,n]\!] \ / \ P^{(k)}(z_0) \neq 0\}$.
   (e) Justifier l'existence de $\omega \in \mathbb{C}^\star$ tel que : $\omega^p = -\dfrac{p!P(z_0)}{P^{(p)}(z_0)}$.
   (f) Montrer que $f : \mathbb{R} \longrightarrow \mathbb{C}$ qui à $t \in \mathbb{R}$ associe $P(z_0 + t\omega)$ admet un développement limité à l'ordre p en 0 et le déterminer.
   (g) En déduire que $\left|\dfrac{f(t)}{f(0)}\right|^2 - 1 \underset{t \to 0}{\sim} -2t^p$.
   (h) Conclure.